ERM – a guide to implementation

Note: This Guide is currently in draft form as "work in progress" on which readers' comments are invited.

July, 2009

Executive Summary

This Guide, which is addressed mainly to Board Directors and Senior Executives, sets out the principal points which should be considered when seeking to implement ERM (enterprise risk management) anywhere in the world, in either the public or private sector. It shows that the concept of ERM goes to the very heart of an organisation and that, if implemented in the way we recommend, taking a methodical approach to the management of uncertainty, it will affect the whole corporate strategy and act as a catalyst for radical thinking which actively seeks out both threats and opportunities. The Guide indicates how an action plan can be developed to move towards holistic ERM and away from traditional "silo" approaches to risk management. The implementation process could take time to achieve fully, as it may require fundamental cultural changes affecting behaviour right through the organisation. However, the business will ultimately become much more robust and flexible, whilst optimising the balance between risk and reward. This will give a greater likelihood of continued success, despite the increasing pace of change all around, and great uncertainties and ambiguities about the future.

Key action points for the Board to consider

Our approach to ERM differs fundamentally from many other sources of advice on the subject, because it is firmly based on the reality that great uncertainty about the future exists and takes a systematic and holistic approach to managing that uncertainty. It provides greater control, by supplying additional relevant information on which to base decisions with confidence in a rapidly changing and uncertain world.

Our approach focuses on responding to possible future changes, while recognising that they are uncertain and may well be of greater magnitude or in different directions than we currently foresee. ERM should not only envisage future events or scenarios as far as practicable but study their relationships and underlying causes. Responses to uncertainty should be developed methodically, proactively and holistically, for opportunities as well as threats. We need a high degree of flexibility in our thinking, behaviour, organisation, processes and systems. Crucially, we should seek to make the business itself as robust and flexible as possible, so as to be able to survive threats which are at present unknown or may have greater impacts than expected.

We therefore recommend that Boards should carry out a review of existing risk practices in the organisation (perhaps starting with the brief self-assessment check in Appendix 1) and then if necessary:

1. Introduce (possibly in stages) an ERM Framework which may retain much of the traditional management of foreseeable downside risk events (with amendments where necessary) but goes further and studies and manages the possible future variability of business outcomes, both upside and downside.

2. Ensure that the organisation takes a proactive and unbiased approach to the management of uncertainty, to reduce it as far as it is reasonably practicable to do so, and to develop suitable cost-effective responses to the uncertainty which remains. We recommend the adoption of a methodical, iterative and holistic approach which involves deep thinking about many aspects of uncertainty and the impacts which they

may have on the business, with a view to developing greater understanding, both of individual risks and of the extent to which they are connected with each other.

3. Require particular attention to be paid to areas of incompatibility between the business and the changing outside world, with a view to identifying pressures which may build up and not be recognised.

4. Establish appropriate early warning systems of emerging risks, so that responses can be developed before it is too late.

5. Consider the introduction of quantitative approaches to "modelling" the business, which will enable the risks taken to be matched to the risk capacity, through the exploration of various possible future scenarios.

6. Make arrangements for ERM to be interwoven with corporate strategy and the business development process, and taken fully into account as an important input to them, with the aim of increasing the robustness and flexibility of the business, as well as achieving a suitable risk-reward balance. Pay special attention to the achievement of sufficient financial flexibility to enable the business to survive setbacks which may be more severe than anticipated.

7. Establish an effective and largely independent central risk function, having direct access to the Board when needed, in order to achieve and maintain a holistic and focused approach to the risks for the enterprise as a whole (though the management of the risks will continue to be the responsibility of line managers). If there is already a central risk function, its remit will probably need to be revised and expanded, along lines we indicate.

8. Give inspirational risk-leadership, which is seen to come from the Board itself, and establish the principle in everyone's mind that risk management is about outcome-variability and achieving success, and not only about guarding against the downside possibilities. Allocate sufficient time for risk at Board meetings and, if necessary, broaden the membership of the Board.

9. Establish throughout the organisation a suitable “risk-aware” culture which focuses on opportunities as well as threats, together with a highly developed risk-communication system, embedded risk-procedures and strong risk-governance.

10. Ensure that there are adequate systems in place for identifying, analysing and managing strategic, project and operational risks, both upside and downside, and that these systems are properly integrated.

11. Review the crisis management system and overhaul it if this is needed.

12. Ensure that adequate attention is paid to the views of external stakeholders about the risks which the business faces, and seek to influence stakeholders when necessary.

The Guide expands these action points and outlines how implementation can be achieved.

Contents

Section 4 – Other important activities of ERM

Section 5 – Managing strategic, project and operational risks

Section 1 – Introduction

Why read this Guide?

1. There is evidence that successful organisations tend to have good risk-management practices. For example, this has been found to apply in the financial services industry - see the box in paragraph 52 of this Guide.

> "Enterprises with broader integrated risk management characteristics tend to outperform others in the chemical and petroleum industries". IBM Global Business Services report, *Where there's smoke…* , 2008.

Moreover, it is likely that investors will be looking for companies which have good risk-management practices.

> "We asked whether respondents would pay more to invest in a company with good risk management. Overall, 82% of investors tended to agree that good risk management was worth a premium. 61% of investors could, and did, avoid investing in companies whose risk management they perceived to be lacking." Ernst & Young Survey of 137 major institutional investors, *Investors on Risk*, February 2006.

In recent years a new, broad concept has emerged - enterprise risk management (ERM), which is based on the idea that risks should be looked at holistically across the enterprise, as well as being managed in silos, and that the conclusions reached should influence corporate strategy and the business development process. While numerous businesses round the world have now embraced this new concept, surveys have shown that many of them are finding implementation difficult.

> "Embedding ERM is proving to be a major challenge … Larger insurers are significantly more advanced in most aspects of ERM implementation and are increasingly looking to realise their competitive advantage … In spite of the challenges of embedding in the business, ERM is influencing decisions, with

significant numbers of respondents indicating key business changes in areas such as risk strategy or appetite, asset strategies and product pricing." Towers Perrin report, March 2009, on a global ERM survey of the insurance industry.

Some of the main sources of difficulty in implementing ERM in the financial services industry are known, and it may well be that somewhat similar issues exist in other industries.

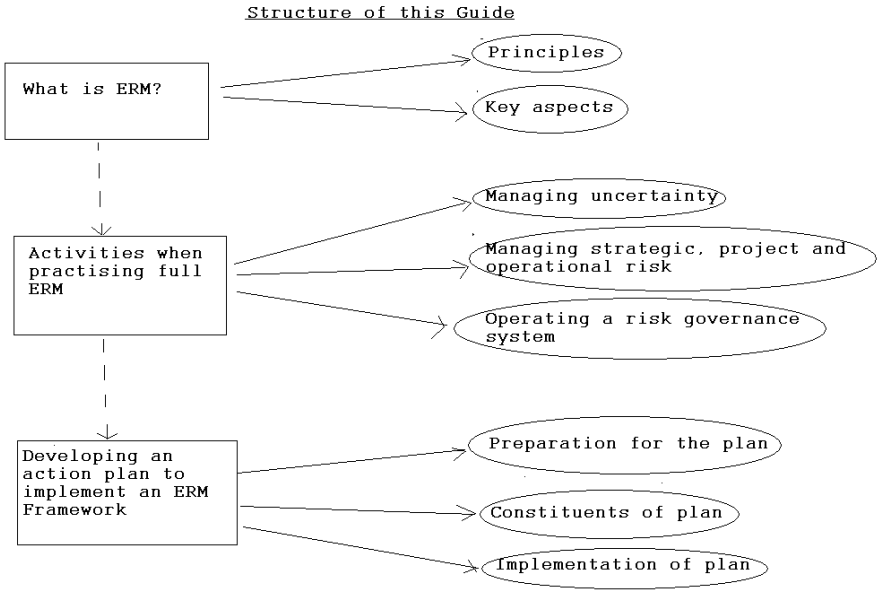
Respondents were asked what were the three main challenges of adopting an ERM strategy and the replies were:

- Embedding risk management within company culture 47%
- Difficulty in quantifying risks 45%
- Timeliness and quality of information 44%
- Difficulty integrating risk management with other business processes 39%
- Lack of necessary knowledge and skills within the organisation 37%
- Corporate priorities are often conflicting 33%
- Availability of information 33%
- It's not clear who is responsible for managing risk 13%

Economist Intelligence Unit Report, *The Bigger Picture*, on a survey of 316 executives from financial services companies around the world in July 2008

This Guide offers practical guidance on implementing and embedding ERM, for Board members and Senior Executives who wish to build on their existing risk-management practices (making amendments to them where necessary) and who are either in the early stages of implementing ERM or are considering the adoption of an ERM approach. Without describing all the tools which are available, the Guide sets out the principal considerations which should be taken into account in constructing an ERM Framework in any business, not only providing a checklist of relevant points but also setting out a practical path through a maze of uncertainties and complexities. It then shows how a suitable action plan can be developed and implemented. We

recognise, of course, that there is a great variation in the types and sizes of the organisations which exist, and that some management boards are more constrained than others. Nevertheless we believe that the principles which are set out here are potentially of very wide application and can be adapted as necessary to increase the chances of success in many different fields of activity. For example, they are just as applicable in the financial services sector as in the construction industry. The Guide offers a comprehensive system to enable the risks arising within an organisation to be methodically and holistically considered, alongside the risks which arise from the organisation's continuing interactions with the rapidly changing outside world. This is just as important in achieving success in the public sector as it is in the private sector. The following diagram illustrates the structure of the Guide:



Section 2 of the Guide describes the main organisational principles of an ERM Framework, including the need for a central risk function which looks at risk holistically, right across the business. In Section 3 we discuss a proactive approach to the management of uncertainty, including a process of radical thinking about the purpose and structure of the business, and its relationships with the outside world, with the aim of providing a useful input to corporate strategy and achieving greater robustness and flexibility. Section 4 describes other important activities within an ERM Framework, including analyses of the capacity of the business to bear risk and the development of suitable risk responses to reduce threats and increase

opportunities. In Section 5 we summarise practical ways in which strategic, project and operational risks can be managed within an ERM Framework, while in Section 6 we set out some important risk-governance principles. Although many organisations will already have risk-management systems which go part of the way towards the processes set out in Sections 5 and 6, we recommend that the existing systems should be reviewed in the light of this Guide and strengthened where necessary. Finally, Section 7 indicates how to get started on an action plan to implement an ERM Framework, though recognising that the plan will differ according to the size and complexity of the organisation. There is also a brief "self assessment check" in Appendix 1.

What is ERM?

2. We have developed our own definition of ERM:

> *ERM is the ongoing proactive process of adopting a holistic approach across the enterprise to all the uncertainty which may affect either positively or negatively the achievement of its key purposes and objectives, leading to action to achieve greater business robustness and flexibility, efficient risk-taking and an appropriate risk-reward balance.*

This definition emphasises ERM as a continuing process which flows throughout the organisation and involves people at every level in it. ERM also helps to set the organisation's strategy and match the risks taken with the organisation's risk appetite, risk capacity and objectives. It does not just seek to identify potential *events* that might affect the enterprise but looks holistically at the relationships between the *system* which constitutes the enterprise and the environment within which it operates, with the following aims:

- to understand as many as possible of the more significant risks which the business faces, and how they are inter-related
- to study a wide range of possible future scenarios and

- to consider how the business might be made more robust and flexible, so that it becomes better able to succeed, even in scenarios which cannot be clearly foreseen at present.

The complex system which constitutes an enterprise has as its heart a group of people whose personal goals will not usually be fully aligned with the goals of the enterprise and who will not normally be in possession of full information - they will therefore react to unusual situations in ways which may be hard to predict. The system can be improved by introducing clear goals and good organisation, training, communication, knowledge sharing and risk governance, as outlined in this Guide. The enterprise operates within an even more complex and unpredictable system - the outside world - and the relationships between the two systems need to be understood as far as possible, even though some of the changes which will take place in the outside world cannot be accurately forecast and may not yet even be glimpsed. Understanding these two systems and the relationships between them, and looking at a wide range of future possible scenarios, will help when devising strategies to make the business more robust, flexible and successful. Moreover, as the recent banking crisis has only too clearly demonstrated, it is not just risk appetite which is relevant, but also the organisation's *capacity* to bear and manage risk.

How does ERM differ from traditional risk management?

3. Traditional risk management operates largely in organisational silos within the business, and studies downside risk without considering upside risk alongside it. It is focused on possible future events, and not on the more general view of uncertainty which is essential for sound decision-taking. It involves such techniques as brainstorming, setting up detailed risk registers of potential risk events, ticking the boxes of risk assurance forms, and making line managers responsible and accountable for the risks in their own areas of operations. For example, a departmental manager may act to achieve safety in the department's own operations, without learning from the safety experiences and precautions of other managers, and without any knowledge of relevant developments in other departments (such as a decision by a procurement department to change the specification of safety equipment purchased). Probabilities and expected impacts of possible adverse events are quantified, often on the basis of flimsy evidence, and risks are sometimes evaluated and prioritised for attention on the

basis of “a probability times impact matrix”, without regard to the fact that a disaster risk may be potentially very significant, even if its assessed probability is small. Estimated impacts of risk events may not take enough account of knock-on effects, such as causing a loss of reputation which then leads to a lack of customer confidence. The underlying causes of risk may not have been studied in sufficient depth to enable those causes to be adequately identified and controlled. Possible responses to specific risks may have been identified in the past but left to remain unimplemented or only partially implemented for reasons of cost. The notions of general responses to risk and built-in robustness are not part of the process.

4. Traditional risk management often places emphasis on the possible occurrence of adverse events, rather than on scenarios which might have a range of consequences, both positive and negative. Uncertainty which cannot easily be envisaged or measured is put in the “too difficult” category and largely ignored, even though its consequences might well affect the organisation more in future than the event-risks which are studied in great detail. Managers at the centre of the organisation may not be aware in a timely enough way of new risk trends which are apparent to staff in outlying business areas. There is usually no comprehensive system for communicating with employees in general about risks and involving them and seeking their help. The Board is often too busy to spend much time on risk and relies on Senior Executives to alert it when things start to go wrong, even though it may then be too late for effective action. Many companies have found that traditional risk management can be misleading by providing false reassurances, or it can fail to provide sufficient insights about the true and developing nature of risk and give only a shaky foundation on which to make decisions.

5. The crucial point about ERM, on the other hand, is its holistic and unbiased nature. It requires the Board itself to give adequate time to consider risk and to give risk leadership for the business as a whole. It brings together through a central risk function the vital work undertaken throughout the organisation on managing risk, and adds an extra “corporate” dimension which enables the Board to better understand the totality of the risks and uncertainties which the business faces, and the actions which could be taken in response to opportunities and in mitigation of downside risks. ERM also seeks out any underlying causes of risk which might cause a number of

problems to arise at the same time in different areas of the business, and looks at how different risks are connected with each other. When fully implemented, ERM ensures that emerging risks are identified as soon as possible in order to give enough time for responses to be developed.

6. One of the benefits of ERM is to indicate possible strategic changes of direction to make the business more robust and flexible, given the great uncertainties about future external changes. This approach to risk helps the Board to do its job of making good strategic decisions and choices, as well as to assess the organisation's overall need for capital and to improve capital allocation within the business. In determining the organisation's responses to risk, the Board will seek to achieve an appropriate risk-reward balance, having regard to the need to achieve risk efficiency by controlling downside risks sufficiently and optimising upside risks, whilst not incurring excessive costs in doing so. ERM places emphasis on managing opportunities as well as threats, by strategising to create value, and thereby enables the whole risk management process to be seen in a positive light and perceived as crucial to the success of the business. Many of the practices of traditional risk management will be retained, with suitable amendments to place them in a new holistic context where knowledge of risks is shared. In particular, despite ERM's greater emphasis on general uncertainty and the properties of the business system and its relationships with the outside world, it will still be necessary to identify and manage some foreseeable risk events. There will also continue to be a need to monitor and analyse risk events as they occur, partly in order to learn how they have been dealt with but also with the objective of identifying patterns which may increase understanding of changes in the underlying business system and its external relationships, or which may give an indication of pressures which are building up. Risk governance may need to be strengthened.

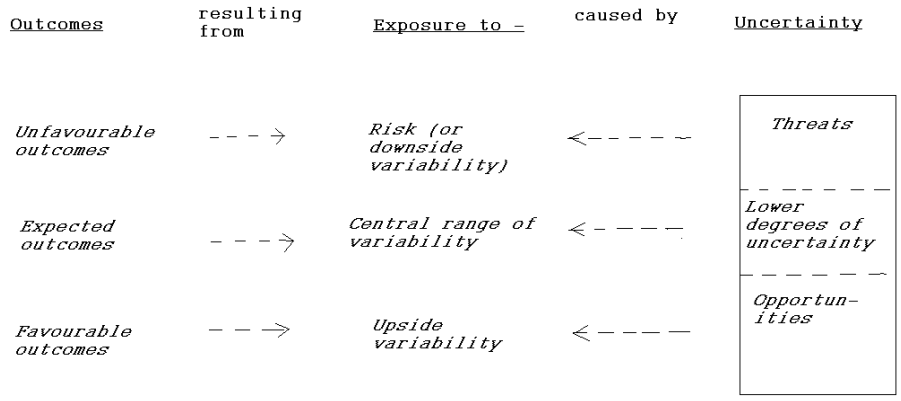
7. ERM requires clear thinking and a sound understanding of the organisation and its place within the outside world, and it is not an easy task to ensure that this is fully achieved and that forecasts and risks are properly evaluated and prioritised. Cultural changes and training may well be needed before employees in general can be sufficiently involved. Hence one of the aims of introducing an ERM Framework such as that set out in this Guide is to enable a business to organise its risk

management effectively, right across the organisation. ERM may involve extra work, compared with traditional risk management, though this is not necessarily the case if some of the existing risk practices can be abandoned (as mentioned in paragraph 78, for example). It is essential that the whole ERM process is thought through carefully in a structured approach, so that it is properly oriented towards achieving results which are useful in practice. As part of the clear thinking process, there is a need for clarity about the meaning of the language used, and definitions of all the principal terms we use are given in the Glossary. By "downside risk" (sometimes shortened to "risk"), we mean exposure to unfavourable outcomes, while the term "upside risk" means exposure to favourable outcomes. The division of prospective outcomes into unfavourable, expected or favourable may be assessed quantitatively, as the extent to which an outcome exceeds or falls short of either an expected value or a target value, or qualitatively, as the extent to which it is judged that the outcome would be beneficial or deleterious. However, the actual perception at the point when the outcome actually occurs (if it does) may well be different. Even at the present time, perceptions about whether specific outcomes would be favourable or not may vary from one person to another, depending on their expectations and objectives. (Also, a particular outcome may sometimes be seen as favourable in some ways and unfavourable in others.) This doubt, about whether certain outcomes would be favourable or not, is one of the components of uncertainty which makes ERM complex. For example, a delay in getting planning permission for an important project may be perceived at the outset as unfavourable, yet it could turn out to be an opportunity to incorporate beneficial new technology.

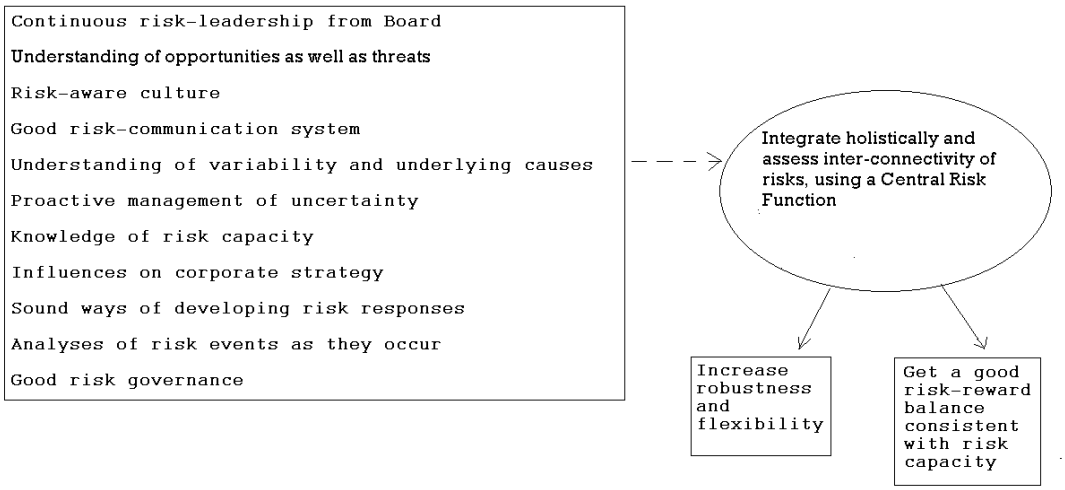
> "Risk solutions are three parts opportunity and one part downside protection" - Greg Case, CEO of Aon

The ways in which various kinds of outcome result from different aspects of uncertainty are illustrated in the following diagram:

How outcomes are influenced by uncertainty



The next diagram illustrates the ERM process and some of the principal activities which we envisage taking place in a fully-functioning ERM framework:



The ERM Process

How are we qualified to offer guidance?

8. This Guide is produced by a working party of actuaries, civil engineers, academics and consultants, who between them have wide experience in risk management [see Appendix 2]. The group came together under a long-standing joint initiative between the actuarial and civil engineering professions in the UK, which aims to develop new and effective ways of managing risk. The initiative has already resulted in the publication of guides to the management of strategic risk and project risk [see the first two items of "selected further reading" at the end of this Guide] and work has also been undertaken on operational risk in some major industries. This ERM Guide builds on that existing knowledge and guidance. The principles set out in the Guide have been tested to a considerable extent in practice, though systematic integration of the principles, as we recommend here, is rare and some of the tools mentioned are still evolving.

Section 2 – Organisational principles of an ERM Framework

Board leadership

9. A key requirement for an effective ERM Framework is effective and ongoing risk leadership from the Board itself. The Board needs to give adequate time to ERM, on a regular basis, and to ensure that the various parts of the Framework are fully in place and operated in a timely and effective manner.

> "Almost nine out of 10 companies have some board-level involvement in their current approach to risk management." Aon Global Risk Management Survey, 2009, which was based on replies from 551 respondents covering a broad range of industry sectors around the world. This useful survey also revealed, however, that in only 15% of cases did the Board systematically participate, while in 32% they considered specific business risks, in 42% they reviewed risks annually (or periodically), and in the remaining 11% their involvement was none or unknown.

10. The reasons why the Board itself needs to be fully involved in the risk management process are because:

- It is usually only at Board level that a sufficiently holistic approach can be taken to the management of the risks, bringing together and prioritising the major risks in various parts of the business and making the connections between them in a "joined up" way
- The Board, working collectively, is likely to be multidisciplinary and have longer and broader experience than most individual Senior Executives (although more non-executive directors may need to be appointed to achieve this fully)
- It is the Board which has the authority to ensure that risk management is given sufficient attention throughout the business, despite other pressures.

> "Two key pillars are emerging as supporting components of ERM: risk culture and governance, and risk-based decision-making." – Towers Perrin website, *Step by Step: Assessing Your Company's Risk Culture*, 2009

11. Real commitment and leadership are needed to ensure that an ERM Framework is devised which meets all the necessary requirements, as outlined in this Guide, and that it is properly implemented throughout the organisation. The Board itself should take ownership of the process, though one designated member of the Board will normally have special responsibility for implementation. Depending on how the business is organised, this Board member may well need to be supported by a Central Risk Function, as described below.

12. It is the Board's responsibility to understand the overall risk picture and the possible impacts on the business. The Board should then give risk guidance to the rest of the organisation. (One of the tools which may be useful to encourage a shared understanding of the main risks and to monitor change is some kind of "risk map"). All Board members should have a good grasp of the general nature of risk and uncertainty, and the processes available to manage them, as well as knowledge of the proven dangers of "groupthink" and the reasons why bias can occur in risk assessments. The Board should identify shortlists of key strategic threats and opportunities, and develop a strategy for focusing on them, supervising their management effectively on a real time basis, and ensuring that they receive continued and sufficient attention. The Board should also put adequate processes in place for positive assurance, regulatory compliance and governance. Where governance issues are raised, the Board needs to ensure that they are given sufficient attention in a timely way, and where these issues appear to conflict with short-term business objectives, the Board must take great care if there is any question of over-riding the governance issues for a while.

Culture

13. It is the Board's responsibility to ensure that the organisation has a culture which is conducive to risk management, with consultative leadership, participation in decision-making on risks, openness, accountability rather than blame, organisational learning, knowledge sharing and good internal communication. The objective is to create an aware, intelligent and responsive business. Everyone in the organisation should participate in one way or another, so that the Board remains fully informed of important developments at the earliest possible stage. Risk management should be

regarded as helping to achieve success and not as a box-ticking exercise designed to protect Senior Executives from criticism or to satisfy regulatory requirements. There should be a widespread recognition within the organisation that ERM is not about avoiding risk - risk and reward are essential elements in running a business - but about choosing the risks which the organisation accepts (for both threats and opportunities) and managing them well.

Some questions to ask about an organisation's culture:
Is there a general pro-active risk-aware culture at all levels? Are staff encouraged to challenge existing practices? Do staff feel able to raise risk issues (even if "bad news")? Are staff encouraged to seek out opportunities? Are staff confident that they will not be blamed for failure when risks have been well managed? Is there an oppressive culture that inhibits learning from experience? If success is to be rewarded, how is success defined?

Although the intricacies and implications of uncertainty need to be understood and acted upon by senior management, such difficult issues need not concern the majority of staff, who will help just by becoming risk-aware and communicating freely about the threats and opportunities they perceive. ERM should be integrated smoothly into their everyday work in a simple way, so that it does not distract them from their main jobs. They will then be pleased to be able to make inputs which are seen to be appreciated and useful.

14. There may sometimes be a degree of tension between the culture which the organisation has developed for growing its business and the culture which is most suitable for managing enterprise risk. For example, a company may be pursuing an aggressive "can do" culture, which is resulting in rising sales and profits, higher rewards for staff, bold initiatives and satisfied customers. Anyone who is highlighting threats or bearing bad news may be silenced or even dismissed unless an

appropriate culture exists. The governance arrangements need to be sufficiently strong to ensure that risk warnings can be issued without fear of victimisation or dismissal and cannot be over-ridden by one individual acting alone. Everyone should be brought to realise that having a risk-conscious culture alongside the "can do" culture is appropriate and necessary, since it embraces opportunities as well as threats and increases the chances of success in the end.

The Board of HBOS, a major UK banking group that was pursuing a vigorous growth policy, dismissed its head of group regulatory risk in the autumn of 2004. He then made a number of allegations about his successor and the bank's overall risk framework, which were followed up by the bank's regulator, the Financial Services Authority. After a full investigation they concluded that some of the allegations were unfounded, but they continued to pursue concerns about the risk management framework. In particular they concluded that the group risk functions still needed to enhance their ability to influence the business, which they saw as a key challenge. In June 2006 they wrote to the bank, making it clear that (whilst the group had made progress) there were still control issues, that the growth strategy of the group posed risks to the whole group and that these risks must be managed and mitigated. However, in the autumn of 2008, following the onset of the worldwide credit crunch, the Bank collapsed and had to be rescued, with great loss to its shareholders and burdens for taxpayers

- Summary based on FSA statement dated 11 February 2009

Communication

15. ERM requires a great emphasis on the use of internal communication to ensure that the identification, updating and management of the more important uncertainties and risks take full account of a variety of ideas, perceptions and experience within the organisation. The sources of uncertainty can be complex and may be hidden from people at the centre. Everybody in the organisation should therefore have an

accountability to identify risk (both upside and downside) and report accordingly. A transparent approach to risk which involves staff and values their views on threats and opportunities can be hugely energising for them (as we found when visiting a transport organisation which already practises such an approach). It can also lead to a more objective process for allocating resources to control risks. Even staff who are not responsible for the management of a threat or opportunity they have identified should be encouraged to think about its management and make suggestions. Staff should be particularly concerned with the areas in which they themselves work, but they should not feel constrained, and should be encouraged to think about threats and opportunities in other parts of the organisation and in the business as a whole. Employees need to be fully aware of where their views and suggestions on risks can be sent, and it should be understood that no blame will be attached to them for communicating in this way, even if they are mistaken or if they offend someone else in the organisation by doing so. The reporting mechanism needs to be such that the communications on risks received from staff are not only reported to the line manager concerned but can also be collated at a central point, where they can be put alongside reports from other staff and understood in the context of the business as a whole.

> "Too often, unwelcome surprises come from risks that were known somewhere in the organisation but were never made visible at higher levels of the business." – *Risky Business*, Conference Board Report, 2007.

One important aspect is that there needs to be a common language about risks throughout the organisation, to minimise misunderstandings and ensure accurate communication. This language needs to fit the wider language commonly used within the organisation.

> We were impressed by a transport organisation's common risk language that has the great practical advantage of simplicity. All risks are categorised as 1,2,3 or 4 on the basis of the required action and management attention. A P1 risk is a "very high project risk", an O3 risk is a "medium operational risk" and a B2 risk is a "high business risk". There are formal qualitative

definitions of these four levels and this language is used throughout the organisation, immediately communicating risk understanding.

Moreover, the leaders of the organisation need to communicate their basic policies and assumptions on risks to all staff (whilst making it clear that these assumptions can and should be challenged if necessary), so that relevant communications in both directions can take place within a shared context, and decisions throughout the organisation can take account of the risk policies which have been adopted at the centre. For example, it is very likely - and appropriate - that an organisation's policy is that staff safety should always take precedence over financial considerations, but this key value needs to be communicated so that those members of staff , at all levels, who are trying to minimise cost buy into the policy fully and reflect it in their own decisions.

"Risk management is ultimately about people" - James Lam, *Enterprise Risk Management from Incentives to Controls,* Wiley, 2003

16. Everyone needs to be aware that there is often evidence available which could alert the organisation to the fact that an important risk is "brewing". For example, there may be:

- A change in observed trends in aspects of the operations
- Changes within the relevant industry, which have not yet affected the organisation but which are starting to impact on competitors
- A series of apparently localised and unconnected events which, if considered together, would indicate an unexplained underlying change.

Such information needs to be gathered, filtered, categorised and reported, and connections made between factors that could combine in order to cause major overall risk. It is vital that the Board understands in a timely way the significant or potentially significant events happening in all parts of the organisation, while overseeing the management of the most important risks itself. There needs to be an openness which enables risk issues to be communicated upwards, downwards or sideways, and an easy reporting mechanism on such matters as

- Perceptions of new or enhanced threats and opportunities
- Suggestions for mitigation of threats
- Ideas for increasing opportunities
- The existence of defective procedures
- Failure to operate established procedures properly.

> In a report of the prosecution which followed the Hatfield rail crash on 17 October 2000, with 4 deaths and 102 injuries, it was stated by the prosecutor that the rail which broke, causing the crash, was first identified as suffering from fatigue about 21 months earlier. By February 2000 it urgently required replacement and another rail was sitting beside the line waiting to be fitted at the time of the crash. He said, "It had been there since April 22, yet despite the danger the track posed, no speed restraint was put in place - this simple measure would have avoided the derailment and crash." - *Mail Online Report*, 31 January 2005.

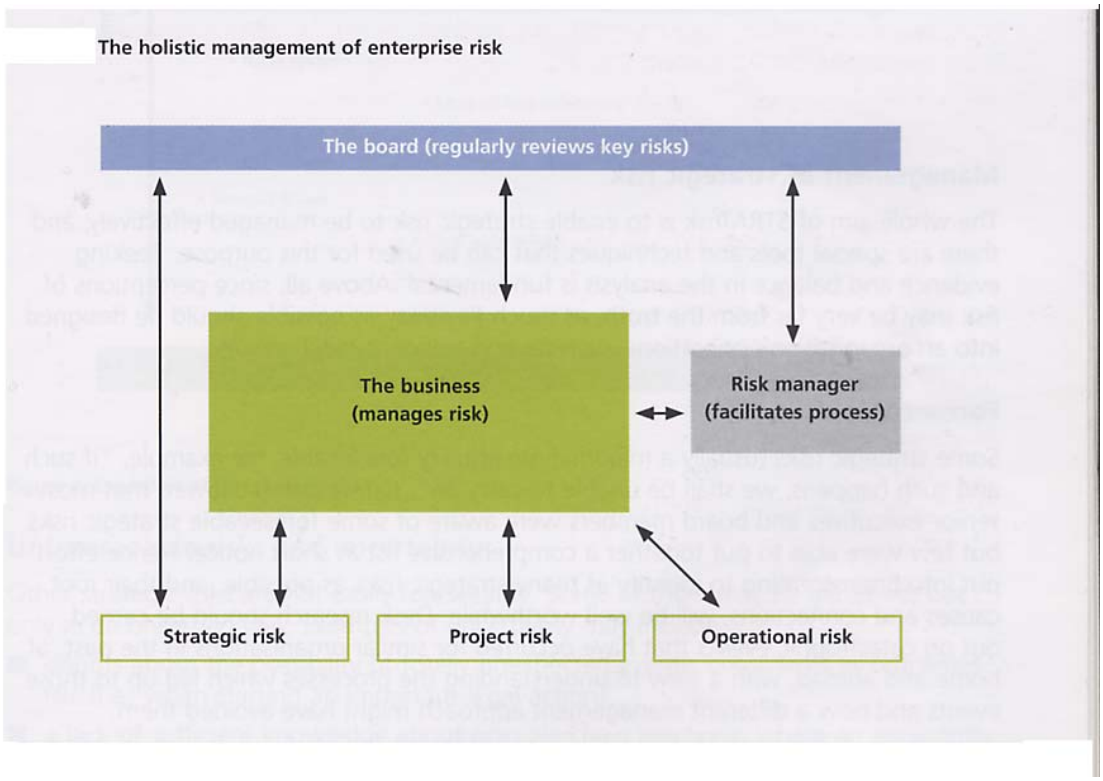
17. To achieve all the necessary cultural and communication goals, some organisations may have to go through a substantial change programme, with training and coaching for all employees. This could take considerable time, effort and expense, but may make all the difference to success or failure of the business in future. It is important to ensure that everybody, at all levels, understands the organisation's risk strategy and how their own responsibilities and functions relate to it. Clarity of communication is a key requirement of ERM, and there must be a mechanism which distinguishes the important communications on risk from the overload of emails and circulars with which employees are bombarded daily. Internal web-based networks can be surprisingly powerful for sharing knowledge if they also offer the facility to put questions and receive speedy and relevant answers, though it is not sufficient to put risk policies on an internal website and hope that employees will access it, unless they have an incentive to do so. Employees' understandings of risks, and their attitudes towards reporting risks, should be tested regularly, with the aim of achieving gradual improvement. Employees who make reports on risks should always be thanked for their trouble, and at a later date they

should be given an explanation of what, if anything was done or not done, and why. If one part of the organisation encounters new risks, those risks need to be notified promptly to managers in other parts of the organisation which may also encounter them. The same applies to successful risk management actions adopted in one part of the organisation, which may be beneficial if adopted in another part.

18. Communication with suppliers and customers about risks can be equally important, even if the message is unpalatable. This should be two-way communication and may alert either side to risks they have not fully perceived. Misunderstanding by either side of risk priorities might sometimes lead to serious mistakes, or to insufficient controls being applied to risks which are important. In the case of suppliers, it is necessary to understand whether they, too, have an effective process in place for controlling their own risks.

Organisation for managing risk

19. The Board must give itself enough time to manage the highest level of the risk process effectively, with challenging reviews and annual in-depth discussions. Unless the process is formally established, short-term business and financial issues can easily distract the Board's attention from emerging risks. Yet there is a need to strike the right balance and not make the process a bureaucratic one. The Board should establish an effective holistic system of ERM meeting its own requirements, to study uncertainty and to manage strategic, project and operational threats and opportunities. To assist the Board and add the vital extra "corporate" dimension which looks at the enterprise as a whole, there needs to be a Central Risk Function or equivalent, which will carry out many important risk functions (see paragraph 20). The risk management processes should be embedded in the mainstream management processes of the business, becoming part of the normal way of life for line managers. The following diagram shows one possible "good practice" framework for ERM:



In this diagram all of the risks, even the important ones, are managed by line managers and project managers within their own spheres of responsibility. However, the Board as a whole will supervise the management of the more important strategic risks and the whole area of general uncertainty. The Central Risk Function (represented in the diagram as a risk manager) will facilitate the process and advise the Board, but will not actually manage the risks. (Although for simplicity the three categories of risk are here shown separately, in practice they overlap - a more detailed description of each category and the management of their risks is dealt with in Section 5).

The Central Risk Function

20. Many businesses already have one or more managers at the centre who are specifically charged with a number of responsibilities relating to risk, but often these responsibilities fall well short of those required for full ERM. We recommend that every business which wishes to adopt ERM should have a Central Risk Function (CRF) at its heart, charged with the wide-ranging responsibilities set out in paragraph 21. In a small business, the CRF might consist of part of the time of a full-time Senior Executive, while in a large and complex business the CRF might consist of a

full-time Risk Manager and staff. However, in those cases where there is no separate risk function, and risk management is the part-time responsibility of a senior executive such as the CFO or CEO, the danger is that other pressures will crowd out essential risk-management tasks. We recommend that fragmentation of the CRF role between different central departments should be avoided where possible, since this could hinder the taking of a holistic approach. There needs to be a person or group of people, below Board level, who have sufficient time and expertise to carry out a range of risk-related functions properly, and in an unbiased way, as it is only by doing this that there can be an adequate focus on the overall risks facing the business as a whole. They must be led by a person who has an independent mind and a challenging and imaginative "best practice" approach to risk, allied with the necessary diplomatic skills, and who has sufficient stature within the organisation for his or her views on risk to be weighed appropriately. We do not believe that all organisations necessarily need a separate post specifically designated as "Chief Risk Officer" or "Head of Risk", but we do consider that where there is no such post the Board needs to ensure in other ways that the necessary holistic approach is taken and that the tasks listed in paragraph 21 are carried out in a suitably "joined up" manner.

> "Having a single view of risk is critical to making consistent and informed decisions. When risk management is siloed, without one person or team owning the process, no one has visibility to aggregate exposures and accountability for the decisions, and risk interrelationship cannot be easily identified." John Farrell, KPMG's lead partner for ERM, KPMG press release, 20 January 2009

Whatever form the CRF takes, it needs to have a recognised leader, and he or she must have personal access to the main Board and the CEO whenever necessary. When talking to investors, it is important that the CEO is seen to be taking ownership of risk. The disadvantage of the CRF forming part of the Audit department is that the internal audit function should extend to the audit of the risk management processes themselves – however, there needs to be a good partnership between the Audit department and the CRF, to prevent unnecessary duplication of effort or gaps. In the case of very large organisations, it may be considered desirable to set up risk

functions in each of the businesses or regions, in addition to the CRF. If so, there needs to be effective liaison, with transparency and adequate reporting to the CRF on all important matters - see paragraph 92 for an example of a failure to achieve this. It is sometimes argued that having a CRF carries the danger that the rest of the organisation may become less involved with risk and less committed to its effective management, because of a mistaken perception that risk is all being managed centrally. This danger needs to be faced head on, with clear communication about the role of the CRF and an understanding throughout the organisation that its functions are additional to, not instead of, the risk management functions being carried out by line managers and project managers.

"The board of a BOFI [bank or other financial industry entity] should establish a board risk committee separately from the audit committee with responsibility for oversight and advice to the board on the current risk exposures of the entity and future risk strategy….. In support of board-level risk governance, a BOFI board should be served by a CRO [chief risk officer] who should participate in the risk management and oversight process at the highest level on an enterprise-wide basis and have a status of total independence from individual business units. Alongside an internal reporting line to the CEO or FD, the CRO should report to the board risk committee, with direct access to the chairman of the committee in the event of need. The tenure and independence of the CRO should be underpinned by a provision that removal from office would require the prior agreement of the board."

- extract from Sir David Walker's report of 16 July 2009, *A review of corporate governance in UK banks and other financial industry entities.*

21. The responsibilities allocated to the CRF (whilst not including the actual management of risks) should be far-reaching and will normally include the following:

<u>Giving strategic advice</u>

- Identifying the organisation's risk appetite and risk capacity

- Facilitating the process of "thinking the unthinkable" about serious business uncertainties and how the organisation should be positioned to meet them, using scenario analysis and other tools
- Understanding the pressures (sometimes hidden ones that need to be sought out) which might build up and suddenly have a major impact on the business
- Integrating all the risks across the business in a suitable way, making connections between different risks, comparing the totality of the risk taken with the risk appetite and risk capacity, and recommending actions to deal with any mis-match
- Carrying out scenario analysis and stress testing for the business as a whole, possibly with the use of quantitative models where appropriate [see paragraphs 49-52]

Studying causes of risk

- Studying underlying causes of risk in various parts of the business, using pattern recognition, concept mapping, brainstorming, workshops, and historical data on risks which have arisen in the past or elsewhere, so as to identify hidden risks, as well as risk connections and any underlying causes which might give rise to a number of risk events occurring simultaneously in different parts of the business
- Sponsoring studies of risks already embedded within the organisation [see paragraph 66]

Keeping track of emerging risks

- Ensuring that there is a sharp focus on emerging risks [see paragraphs 44-46]
- Acting as a central reporting point, to which any staff members (not just managers) may communicate emerging risks and their comments or concerns on threats and opportunities

Acting as a source of good practice

- Seeking to benchmark the organisation's risk-management practices against the risk-management practices adopted by other organisations

- Becoming a centre of excellence for guiding line managers and project managers on suitable techniques for identifying and managing risks and uncertainties (having regard, for example, to "risk efficiency")
- Making recommendations for practical procedures to manage strategic, project and operational risks [see Section 5]
- Advising on the actions which need to be taken to introduce good risk governance mechanisms [see Section 6]
- Introducing a common language about risks throughout the organisation and ensuring the continued effectiveness of risk communication in general [see paragraphs 15-18].

Other activities

- Monitoring managers' progress on taking actions to respond to risks in ways which have been agreed
- Helping to place financial values on risk where appropriate and practicable
- Briefing regulatory authorities, credit rating agencies, share analysts and other external parties on the systems which are in place and being developed for managing risk.

Many of these tasks will, of course, be carried out in conjunction with line managers and project managers, while others will involve discussions at the Board itself. Some of the tasks are considered in greater detail in the following Sections of this Guide.

> "For a truly enterprise wide risk management approach, the Head of Risk should ensure there is consideration across the entire portfolio, including all broad risk categories, be they internal or external, operational, change related or emerging and strategic in nature." KPMG Report, *The Evolving Role of the Head of Risk*, 2009

Section 3 - Managing uncertainty

What is Uncertainty?

22. Uncertainty is a key concept in this Guide, meaning incomplete knowledge, i.e. a shortfall of knowledge or information about:

- what kinds of outcome may occur,
- the factors which may influence future outcomes,
- the extent to which known and unknown factors will influence outcomes,
- the likelihood of various outcomes,
- the impacts which those outcomes, if they occur, would have on the organisation.

Uncertainty may lead to a lack of sufficient control of the enterprise, and should therefore be minimised as far as it is reasonably practicable to do so. In an ERM environment considerable management effort will be devoted to reducing uncertainty, which will usually be undertaken in successive steps. Eventually a point will be reached where it is not considered worthwhile at the present time to seek to reduce uncertainty further, and for practical purposes some assumptions may then have to be made about the residual uncertainty which remains. However, it should always be remembered that these areas of residual uncertainty may affect outcomes in ways which differ from the assumptions. Uncertainty may, of course, be reduced further at a later date, through the discovery of further knowledge or information, and ERM requires some management resources to be devoted to the discovery process. Inevitably uncertainty will include some really major future possibilities which can only be glimpsed or may be totally out of view. However, a methodical and focused approach to uncertainty can reduce its negative impacts and improve its positive impacts, thus increasing the chance and degree of success.

23. At least four kinds of uncertainty may be distinguished and these may be useful subdivisions within which to analyse uncertainty in a particular context or to understand what aspects of uncertainty have already been addressed:

- Event uncertainty - good and bad occurrences or scenarios that may or may not materialise;

- Variability uncertainty - variations in outcomes that are expected to occur but to an extent which cannot be forecast accurately;
- Assumptions uncertainty - the extent to which any implicit or explicit assumptions which have been made to fill in knowledge gaps may or may not turn out to be true. For example, most sources of uncertainty are not entirely independent of other sources, even though this may often be assumed for simplicity.
- Systemic uncertainty - relationships, which are usually themselves uncertain, between different sources of uncertainty, including "knock-on effects".

Some aspects of uncertainty relate to whether particular forecast numbers are likely to come approximately true, or to the possible range of variation in those numbers, but other aspects concern much broader relevant considerations that may be unquantifiable but still need to be taken into account.

Uncertainty is a perception, and what may be uncertain to one person may be less uncertain to another. For example, an experienced manager in a financial services business might find it easier than would an inexperienced colleague to appreciate the extent of possible variations which might occur in the investment climate. This suggests that uncertainty is probably most effectively studied by a group of people who have a variety of experience, including some who come from outside the industry in which the business operates. Recent experience, or experience restricted to a single industry, too often restricts the vision of possible futures. There is usually a real need to "think the unthinkable" before a realistic range of possible futures can emerge. Uncertainty also includes the general "fuzziness" which often surrounds some of our thinking about the probabilities and impacts of those risk events which we can foresee as possible occurrences – we may think we can estimate these probabilities and impacts approximately, but there is usually an imprecision about these estimates, and the margins of error may be wider than we believe. In some organisations there may be uncertainty about the objectives of the organisation or its risk capacity, and the possibility that these may change in future, for example if there is a new government or a less ready supply of credit. There may be uncertain or unintended consequences of management actions - for example, adding more people to a software development

team when a big software project is in trouble has been equated to trying to put out a fire by pouring on petrol. The knock-on consequences of major incidents - e.g. serious accidents - may be hard to predict, and may be wider than could reasonably have been expected. The complexities and ripples of uncertainty are great, and the intellectual thinking power which is necessary to cope adequately with it on an ongoing basis should be seen as a key asset of the organisation, and not just as a resource which can be brought in from outside when necessary.

An approach to uncertainty management

24. Since uncertainty is so complex, is it feasible to manage it proactively, or must we just accept that it exists and do the best we can in spite of it? We firmly believe that the former is the case, and that a proactive, focused approach to the management of uncertainty can be one of the most important drivers of future success, by capitalising on opportunities as well as coping with threats. For those areas of uncertainty where we think it might be possible to reduce our lack of knowledge, we should aim to do so, as long as we believe that the further effort is worthwhile and cost effective, having regard to the potential benefits. To cope with the remaining areas of uncertainty, we should aim to adjust the business strategy, so as to make the business more robust and flexible, and able to survive and achieve success, whatever the future may bring.

25. In seeking to manage uncertainty we should aim to gather as much information as we reasonably can which is or may be relevant in a significant way to the organisation's business.

> "Lack of knowledge is the greatest challenge to overcome related to business interruption risk." Aon Global Risk Management Survey, 2009.

Given the mass of information which exists, much of which may turn out to be immaterial to the business, it is essential to follow a structured and iterative approach, which gradually focuses in on key and relevant information but ensures that wider relevant information is also taken into account, without closing down the search for

additional knowledge too soon, as can so easily occur. One way of doing this is to proceed in the following way:

Step 1: Assess what we think we know already.

Step 2: Assess what we know we don't know and systematically gather further information to fill the gaps to some extent.

Step 3: Assess the extent to which all our knowledge may be "fuzzy", i.e. imprecise or not properly understood, and gather further data to reduce the fuzziness.

Step 4: Conduct a broad thinking process to identify additional areas of knowledge which may be relevant to the business, including information about the future which we can just glimpse or even perhaps not be able to see at all (but excluding information which is clearly not relevant), and carry out an analysis of it to identify which areas can safely be discarded and which must be retained as relevant even if much of the knowledge in the areas concerned remains hidden. Set in hand a process to gather further information, if possible, in the retained areas.

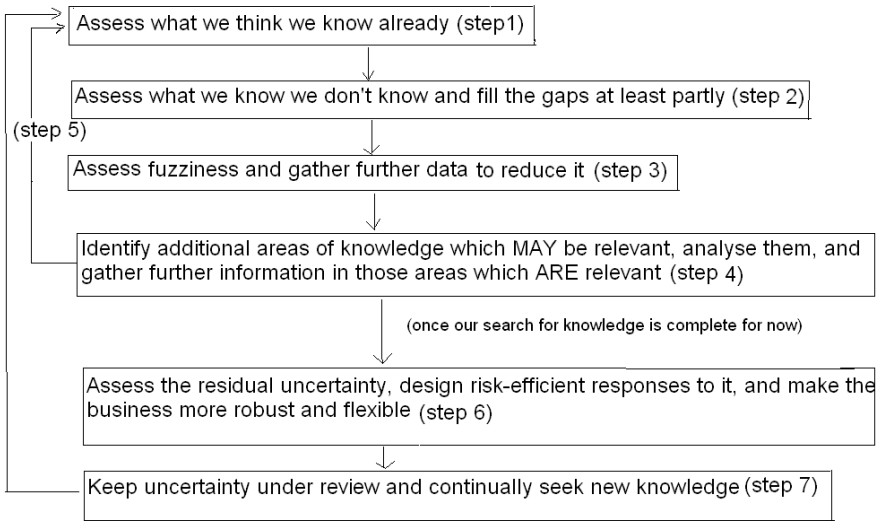
Step 5: Go back to step 1 and repeat the loop, gradually focusing in on key information which appears to be relevant, until a point is reached where it does not appear worthwhile or cost effective to seek to acquire further information at present.

Step 6: Assess the residual uncertainty, and design and implement responses to it which satisfy the principle of risk efficiency. For those areas of residual uncertainty which are relevant but which remain largely hidden, consideration should be given to making the business more robust and flexible, so that it has a better chance of dealing with the unexpected.

Step 7: Keep uncertainty under review and devote resources to a continuing search for new knowledge. As new knowledge is obtained, either through this search process or by accident, assess how far it is relevant to the business, to what extent new risk responses are necessary and whether it changes the strength of the case for making the business robust and flexible.

When analysing knowledge, and deciding whether to discard it or not, it is important to seek out interconnectivities between one piece of knowledge and another, with a view to increasing our overall knowledge and understanding. (Academics are developing mapping tools as a new approach to modelling and visualising the interconnectivity of various risks in an ERM context).

Our recommended process may be represented diagrammatically as follows:



An Approach to Uncertainty Management

As a simplified example of a practical application of this process, consider a hypothetical new underground railway in an urban area, where any future flooding of the tunnel could result in a catastrophic loss of life. At step 1 it is proposed that the tunnel should be designed in such a way as to withstand all floods except those which occur only once in 200 years, based on available past data. At step 2 it is ascertained what flooding data exist over a long period into the past for the area concerned, for both frequency and severity, and any gaps in this data are identified and filled in from data relating to other locations. The data are then used to identify the broad outlines of a design specification (including flood barriers) which meets the "once in 200 years" criterion. Under a traditional risk management process, this might be as far as the matter would go. However, applying our proposed methodology, in step 3 a risk expert points out two flaws in the proposal. First, some limitations in the available past data inevitably mean that the calculated flooding probabilities for the area in question are very "fuzzy" and have a considerable margin of error. Secondly, even if the tunnel could be designed accurately to a "once in 200 years" specification, there would be a 10% chance of flooding at some point in the first 21 years, which is unacceptably high. At step 4, a broad thinking process, involving other experts,

underlines the point that new factors, including intense urban development and climate change, make it possible that the future experience of flooding could be very different from the past experience. Step 5 leads to further research and reveals that experts in Japan, which is in the forefront of thinking about underground flooding, now believe that "variability and uncertainty are becoming the key issues of future Japanese flood management - thinking in static terms of risk has shifted towards an approach where variability needs to be managed" [*Urban Water in Japan*, by Rutger De Graaf and Fransje Hooimeijer, 2008]. This in turn leads to the crucial realisation at step 6 that planning for our new underground railway should not only require it to withstand a reasonable level of flooding but should be based on the assumption that at some point, despite these precautions, the tunnel probably will be flooded. Attention then turns to the ways in which this risk can be managed, including the possibility of building a drainage tunnel beneath the main tunnel. Debate follows over the extra cost that this would entail! As an example of interconnectivity of knowledge, it is important to avoid anti-flooding solutions which increase the fire risk, while conversely it is worth seeking risk-efficient solutions which reduce both the flooding risk and the fire risk at the same time. Once the design has been finalised, step 7 requires the establishment of a mechanism which will keep track of flooding incidents elsewhere and the lessons which can be learned from them in terms of the evacuation of people from flooded underground areas.

This example demonstrates how a structured approach to uncertainty can, in a methodical way, increase our understanding of it and lead to thought about possible responses that might otherwise have been overlooked. Although the example relates to a specific project, exactly the same method can be applied, in principle, to thinking about the uncertainties swirling round an enterprise as a whole.

Ways to reduce uncertainty

26. As part of the systematic approach to gathering information referred to in paragraph 25, the ways in which further information can be gained and uncertainty reduced include the following:

- Definition and acquisition of data which are known to be required

- Research, including a study of similar situations, present or past, in the same or other organisations
- Consultations with experts, including specialists in visualising possible world futures
- Brainstorming and workshops
- Concept mapping for the organisation as a whole to identify key risk areas
- Horizon scanning
- Pattern recognition as events occur
- Consultations with stakeholders (customers, suppliers, staff, shareholders, etc.) and affected third parties, about their views on the business and on likely future developments
- Influencing powerful stakeholders not to act in such a way as to increase the threats which the business faces
- Conducting small-scale experiments, e.g. market testing
- Gleaning as much information as possible about competitors' plans
- Looking for possible ambiguities or incompleteness in the business's success criteria
- Seeking independent assessments of in-house risk appraisals, to eliminate mistakes and bias
- Making a deeper analysis of the business variability and its underlying causes
- Model building, scenario analysis and stress testing
- Financial restructuring

Responses may be developed to both threats and opportunities, in an attempt to reduce uncertainty, but it must be recognised that the responses could themselves create new threats and opportunities.

Assumptions

27. For some practical purposes it may be necessary to make assumptions about the remaining areas of uncertainty. However, we must always remember that these areas may affect outcomes in ways which differ from the assumptions, and it is wise to consider the effect on our courses of action if we were to adopt different assumptions within the range of plausibility.

A well-known example of a mistaken assumption that had tragic consequences was the belief that the *Titanic* was unsinkable and that it was therefore not necessary to provide sufficient lifeboats for all on board.

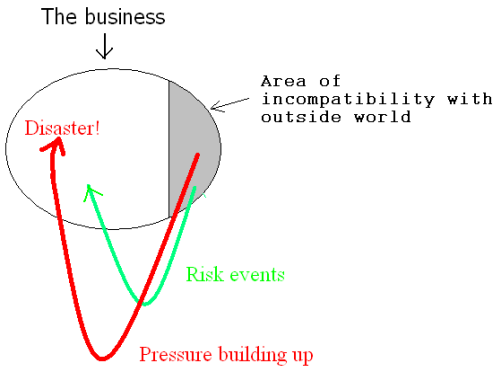
New knowledge

28. At any point of time there are limits to our knowledge and we have to act as best we can within those limits. However, uncertainty may well be reduced at a later date through the discovery of additional knowledge or information, which may then necessitate a reappraisal of variability and business strategy. Such discoveries may be accidental, or they may arise from an analysis of the events which are occurring in the business or in the outside world. They may also arise from further application of any of the proactive processes referred to in paragraph 26. One of the key questions for decision at Board level will be the extent and quality of the resources which are to be put into the ongoing search for new knowledge.

Recognising the need for strategic change

29. A useful concept in the management of uncertainty is to think about a business as a complex system of people, assets, inputs and outputs, which operates within the even more complex system of the world as a whole. There will often be tension between these two systems, which may cause pressure to build up and suddenly result in a major and irresistible impact on the business at some future date. Understanding the nature of the business, and its relationships with the outside world, is therefore crucial, since such understanding could lead to strategic changes in the business which prevent disaster.

30. The following diagram illustrates a possibly disastrous relationship between a business and the wider world in which it operates:



Results of system incompatibilities

There will often be some areas of incompatibility between the business and the wider world, which may give rise to the occurrence of risk events from time to time. The more significant of these risk events should be analysed carefully as they occur, to see if they help to identify any hidden pressures which may be building up. For example, an unfavourable press report about the business may be just the tip of an iceberg of dissatisfaction. It may be years before the pressures reach the point where they get released, perhaps with explosive effect, when it will normally be too late to do much about them. Thus there may be a protracted period during which the business may be able to ignore the pressures without too many adverse consequences, but the outlook may become increasingly dangerous and unpredictable. It is important, therefore, to study any areas of incompatibility with the outside world, even if they do not appear to be seriously undermining the business at present. Recognising potential dangers is not enough, however - action needs to be taken before the tipping point is reached and it is too late. This action may necessitate fundamental changes in business strategy.

31. Similarly the business may not fully recognise its strategic opportunities, which could be lying in wait undiscovered. Again it is a question of seeking further knowledge, but there is also a need to apply a creative thinking process which includes a deep understanding of the environment within which the business operates and the environment into which it could extend.

Changing relationships

32. However, it is not sufficient to restrict our thinking to the relationships between the business and the outside world as they stand today. Not only may the business itself change, but it is certain that the world as a whole will change, and possibly in big ways which will have a major impact on the business. Consideration should therefore be given to possible incompatibilities and new opportunities which may arise in future years. Even if these can only be glimpsed through a mist of uncertainty, this glimpse may nevertheless help in the development of sound business strategy.

> For many years British Members of Parliament were entitled to claim in confidence for a wide range of expenses on production of their receipts. Rules were laid down but a lax culture developed. Although in recent years many other actions of public bodies had become accessible to the public under a new "freedom of information" culture, MPs' expenses remained confidential. However, in 2009 full details of expense claims by individual MPs were published by a national newspaper, showing that many claims had not been within the rules or at least not within the spirit of the rules. Events then spiralled out of control, with a catastrophic loss of confidence by the public, which led to the resignation of some MPs and the Speaker of the House of Commons. A system which had initially been seen as acceptable had become unacceptable with the passage of time, but few had recognised the seriousness of the risks which this created. The underlying cause of the problem was not the event of the leak of information but the incompatibilities of the system. If the system had been changed earlier, the problem could have been averted.

New thinking

33. One of the key concepts behind ERM is that it is worth devoting time, effort and resources to the development of deeper thinking about the purpose of the business, how it interacts with its environment and the wider world, and how it can be made more robust and able to cope with a wide range of uncertain future possibilities. The first task is to "think the unthinkable", i.e. to try to envisage scenarios which might

cause the business to fail completely or might give it the opportunity to perform extremely well, including future environments which are very different from the present and events which (although foreseeable) currently seem very unlikely or far off. One technique in this thinking process is to view the business as a complex, dynamic system, operating within another even more complex and dynamic system. What is it which might cause either of these systems to start operating in a significantly different manner, and what could be the consequences for the business? Managers should be encouraged to think of a multi-dimensional *web* of risk, and not just a two-dimensional matrix of probability and impact – the task is then to identify which parts of the web are relevant. Other techniques to encourage radical thought include thinking from first principles, brainstorming, and actively creating opportunities to "break down the norms" (e.g. by allowing people to write on a blank wall). These processes should be repeated as new insights are gained into the risks and uncertainties which the business faces. In addition it is good practice to have an annual review of the major changes which may lie ahead. It may be useful to gather together a suitable group of deep-thinking and experienced people (including some from outside the organisation), to discuss possible futures. The past 25 years have shown the extent to which major changes can happen in a comparatively short period, and many of the companies which were flourishing earlier in that period no longer exist.

> "Of the 100 companies comprising the [FTSE 100] Index at the end of 1988, only 33 remain. Of the other 67 companies, 15 were either acquired by, or merged with, another current FTSE 100 company, 42 were taken private or acquired by a non-FTSE 100 company, three have been demoted, four broken up and three ceased trading (British & Commonwealth Holdings, Maxwell Communications and Woolworths)." - article by Gary Squires in *The Actuary*, Jan/Feb 2009, page 36.

A good knowledge of historical business or political upheavals, recessions, booms, credit crunches, etc. will help in generating possible future scenarios, since history has a habit of repeating itself, even if the details differ. In particular there is a need to consider relevant extreme historical events or scenarios (possibly many years ago)

whose recurrence may not be beyond the bounds of possibility – managers need to overcome any reluctance to take historical lessons into account because it is inconvenient to do so, and should not automatically believe that history is irrelevant because the world has changed or because of the unique features of the present activity.

Examples of major changes over last 25 years

End of cold war
Rise of international terrorism
Global warming
Increasing life spans and ageing populations
HIV, AIDS, and increasing risk of pandemic virus outbreaks
Unpredicted major developments in IT, telecommunications, internet
Globalisation and greatly increased interdependence of economies
Emergence of giant multi-national companies
New rapidly-developing nations (China, India, Russia and Brazil)
Steep rises and falls in fuel and commodity prices
Energy scarcity
Widespread camera surveillance in shops and public places
Breakdown of banking systems
Global economy going from boom to bust in just a few months
Rapid falls in interest rates to very low levels
Free movement of labour throughout Europe
Emergence of online shopping

One of the consequences of this increasing pace of major change in many aspects of life is that risk management has assumed increasing importance. The strong likelihood of future big changes presents huge and increasing threats, but also great new opportunities. However, there is a need for a different kind of thinking and behaviour if we are to respond effectively to such challenges.

34. Increasingly management needs to focus on dealing with change, both self-created and externally-imposed, rather than concentrating on business as usual. We need to accept that change is the new norm. Hence the management of change and consequent uncertainty must become our main focus. Strategic threats and opportunities should frame the Board agenda. But all levels of an organisation will increasingly be involved in identifying and managing change and the related threats and opportunities. Hence, rather than being an add-on or separate technique to be applied occasionally (as is often the current view), risk management needs to become the very core of management.

35. As currently practised, risk management has a number of serious shortcomings, which prevent it dealing effectively with big changes, notably it:

- Pays insufficient attention to uncertainty, i.e. incompleteness of knowledge
- Treats risk management as if it were a separate activity from management
- Focuses on threats alone, ignoring opportunities
- Concentrates generally on tactical rather than strategic risks
- Tends to under-estimate significantly the degree and speed of potential change.

Why is it that risk management tends to focus on threats to the exclusion of opportunities? Generally this is perhaps because of people's fear or insecurity, or because threats are easier to identify than opportunities, yet even within threats there may sometimes be upside possible outcomes if the risk is managed well. Opportunities require creative thinking to identify and analyse them, but this is worth doing because the potential benefits can be far greater than from managing threats.

36. So what kind of new thinking is required? In summary we must:

- Focus on managing or responding to change
- Take a holistic approach to risk management, covering strategic, project and operational risks and the extra corporate dimension which links them all together
- Adopt a positive approach which focuses on opportunities and seeks the upsides as well as downsides of threats

- Take a higher-order view of threats and opportunities, which is not just focused on possible future events but also considers the possible impacts of broader aspects of uncertainty
- Be highly flexible in our thinking, behaviour, organisation, processes and systems
- Seek to make the business as robust as possible to withstand threats which are at present unknown (or of unprecedented force)
- Ensure that there is a sufficiently wide and creative base of knowledge focusing on future possible changes and on the steps which need to be taken in advance to provide the best chance of managing them successfully
- Ensure that risk management is embedded in the core of all management activity, including the activities of the Board itself.

There was some radical new thinking many years ago about the unreliability of motor cars. Someone came up with the revolutionary idea of adopting a "no tolerance" attitude to manufacturing defects, in order to eliminate the problem. This was an idea which might well have been rejected on the grounds of cost, until someone else suggested that much of the cost might be offset by the consequential manufacturing efficiencies. In the event this proved to be the case and the increased reliability meant that cars became even more desirable purchases than they were previously, which may well have contributed to the enormous growth in the car market since then.

Among other things, there will increasingly be a need to study social and environmental considerations, and the risks to which they may give rise. It is becoming more widely recognised that business activities which are perceived by sectors of the public, or by governments, as socially or environmentally undesirable could result in future pressures which cause great difficulties. (Testing cosmetics on animals is a well-known example).

37. The following table shows a list of some of the major "unthinkable" risks which might throw a business off course or open up opportunities:

Thinking the unthinkable

Threats

New weather patterns - storms, floods, drought, cold winters, heat, infestations
Earthquakes and tidal waves affect UK and Europe
Prolonged shortages – oil, gas, food, credit, trained staff, steel, cement
Nuclear- or bio- terrorism in cities
All UK power stations destroyed in terrorist attack
Political developments severely restrict international trade and off-shoring
New infectious diseases emerge (deaths, loss of workforce, social changes)
World War 3 breaks out
Internet disintegrates
Taxes rise by 50%
Breakdown of law and order
Virus embedded in widely-used operating system destroys most computer programs and data simultaneously
Maximum working week reduced to 40 hours by law
Extreme right-wing Government elected
Massive inflation or deflation
European Union breaks up

Opportunities

Internet makes great technical leaps forward
All new mobile phones incorporate facility to see caller on screen
Tourism to the Moon becomes economical
Cancer and heart disease beaten
Electric cars perform better and become universal
Big infrastructure investment programme (houses, roads, railways, schools)
New carbon-friendly energy sources open up era of cheap fuel and promise an end to global warming
Credit becomes plentiful and property values rise as economic boom returns
Turkey joins the European Union
Tax incentives given to encourage marriage and larger families
Families show greater readiness to save
World disarmament
Robots performing menial tasks become commonplace in everyday life
Far-reaching simplification of statutory rules and regulations
World poverty eliminated

38. This is, of course, a very incomplete list, and nor should all the items on it necessarily be given serious consideration. It is included here merely in order to give

an indication of the breadth of thinking required. For each such risk consideration will need to be given to the possible effects on the business. Indirect effects must also be considered: the occurrence of some of these risks, for example, might result in employees finding it difficult to come to work. Some unthinkable risks will not be of such a general nature as those listed in the diagram, but will instead be specific to the individual business. Moreover, some risks will probably arise in practice which it is quite impossible to even glimpse at present. It is also the case that some of the "threats" might incorporate opportunities and vice versa - for example, changing weather patterns, although a threat to the present ways of doing things, might present opportunities to companies which manufacture weather protection equipment or garments. World disarmament might be an opportunity for world growth and co-operation, but it would be seen as a threat by munitions companies. Thought should be given to how the business might be made able to cope with such situations if they arise, which may well require changes in strategic direction, rather than waiting for the situations to occur, when it may be too late. Such responses will usually be at a very high strategic level, designed to increase the robustness of the business and its flexibility to respond at short notice to unknown future events.

Coping with uncertainty

39. One of the principal aims of ERM is to enable the business to position itself to meet the challenges of an unknown future. Many business risks can be foreseen and appropriate responses can be devised and implemented, covering both action in advance and a contingency plan for dealing with the situation if it arises. However, some of the more important risks are usually totally unforeseeable or can only be glimpsed through a mist of uncertainty. To be in a position to meet these latter risks successfully when they arise may need a great deal of preparation and possibly a change in the overall business strategy to make the business more robust, so careful thinking in advance about what may need to be done for this purpose could be well worthwhile. Moreover, since perceptions of risk may be very far from the truth, and totally new situations can arise very quickly, as much flexibility as possible should be designed into an organisation's operations, systems and response mechanisms. Where, as is often the case, future success depends critically on meeting more than one key objective, the business needs to be robust in respect of all these objectives, which may be difficult to achieve in practice [see also paragraphs 55 and 72].

Modifying corporate strategy

40. The pointers in this Section of the Guide are not, of course, a comprehensive blueprint for corporate strategy, but some considerations which should be weighed up against others when determining strategy. Traditional approaches to strategy include the need to identify what is unique and what is most profitable in the existing activities and then to refocus on the unique or most profitable core and realign the company's activities with it - see for example the article by Michael E. Porter, *What is Strategy?* (Harvard Business Review, November-December 1996) which summarises the recommended approach thus:

> "What approaches to growth preserve and reinforce strategy? Broadly, the prescription is to concentrate on deepening a strategic position rather than broadening and compromising it."

Whilst this now-traditional approach has much to commend it from the viewpoint of growing the business in a competitive market place, it is not always sufficient to enable the business to withstand the pressures of change, either from within or from interaction with the rapidly changing outside world, where we believe that a degree of diversification may sometimes help. Melding the two approaches together is likely to be at the heart of sustained success in future. Although this is a formidable management challenge, we believe that a holistic approach to risk management, as set out in this Guide, will not only enable an enterprise to protect itself against unfavourable developments but will also help it to become more efficient and profitable, and to grow by identifying and exploiting opportunities.

41. This is not the place for a comprehensive discussion on corporate strategy, and in any case each business will differ to such an extent that general guidance will often be inapplicable. However, it is likely that ERM will identify some of the greatest vulnerabilities of the business, and this will help to focus a determined search for strategies which will achieve greater flexibility and robustness. Moreover, ERM may well indicate a wealth of opportunities which could be exploited if a new strategic direction were taken. It is vitally important, therefore, to ensure that the strategic planning and new development processes of the business are fully linked with the ERM process. Some of the corporate strategies which the ERM process could

suggest might include the following, depending on the nature of the business concerned:

- Greater diversification of the business, to achieve a wider spread of risks. (For example some bus companies have diversified into rail franchises).
- Strategies to minimise the impact of reputation risks, for example by adopting different brand names for different parts of the business.
- Financial restructuring [see paragraph 42].
- Renegotiation of arrangements which could prove a handicap to flexibility - for example, costly redundancy agreements.
- Requiring new contracts to contain as may options as possible to achieve flexibility for the business, and as few options as possible for the other party to exercise against the business, even at some extra cost.
- Simplifying the organisation's internal structure and external relationships [see paragraph 43].
- Strategic partnerships to share risks with parties better able to manage them.

Financial flexibility

42. It is often financial constraints which prove most onerous when a business gets into trouble, and in particular the lack of sufficient cash - the liquidity risk. Rather than always seeking the cheapest sources of finance, it is therefore crucially important to retain the maximum possible flexibility on cash, which may one day make all the difference between survival and going under. For example, it may be appropriate to consider the issue of long-dated bonds, rather than relying too heavily on short-term borrowing which might be withdrawn at an inconvenient time. Moreover, it would always be prudent to have a source of additional capital which can be accessed at short notice if cash starts to run out, and which will not dry up when most needed. Even with the best cash forecasts imaginable, there is always the risk of a significant cash shortfall due to the uncertainties surrounding the business. The extent of the financial flexibility which exists may well be a crucial factor in determining the organisation's capacity to take on risk - see paragraph 48. Financing a business can be a complex matter, and there may be a temptation to leave it entirely to experts in the Finance Department, but the key considerations on financial flexibility need to be understood (and if necessary influenced) by the Central Risk Function, which will be

able to achieve linkages with the other areas of variability in the business and enable all the risks to be studied holistically.

Organisational simplification

43. Some of the greatest problems in practice can arise from organisational complexity, which suggests that simplifying the organisation's internal structure and external relationships is likely to improve robustness significantly.

> Catastrophic accidents such as the Bhopal tragedy in 1984, when 16,000 people died because of a release of gas from a Union Carbide plant, and the loss of the Challenger spacecraft in 1986, have been attributed to unmanageable system complexity, while the collapse of the Circle Line Tunnel under construction in Singapore in 2004, with the loss of four lives, was due at least in part to the large number of subcontractors and other parties involved.

This does not necessarily mean that all simplification is beneficial. For example, outsourcing an operation may *appear* to be creating simplification, in that the internal organisation is streamlined, but there are consequential risks, namely liaison difficulties with the other party, problems connected with interpretation of the outsourcing contract, lack of control over the quality of the outsourced product, and problems which might be caused for the main business when things go wrong.

> In 2005 British Airways incurred a £40 million loss due to a labour dispute at Gate Gourmet, the organisation to which British Airways had outsourced its catering operations in 1997.

Early warning of emerging risks

44. One way of achieving greater flexibility is to improve the organisation's ability to see emerging risks at the earliest possible stage, so that there is more time to

develop adequate responses to them, for example by improving communication to the centre from staff in the field who may spot the risks in the course of their work. Having a culture where it is entirely acceptable to report emerging risks promptly is of vital importance. There also need to be procedures which ensure that such concerns are not then ignored at the centre, unless they prove groundless. Clustering and organisation methods need to be in place, so that the process is not overwhelmed by a mass of information. Particular attention should be paid to the possibility that a chain reaction is starting – small events that could lead to dangerous escalation. In addition there should be a structured system of horizon scanning at the centre of the organisation, trying to spot unexpected big issues, threats and opportunities that may be "coming over the horizon" – new legislation, changing financial and economic conditions, emergence of competition, technological change, etc.

Horizon scanning issues

How often to scan?
Length of time ahead for which the horizon is to be scanned?
Width of the field which is to be scanned?
Scanning for opportunities as well as threats?
How far can information technology be used for scanning?

- Summarised from *The Orange Book*, HM Treasury, Oct 2004

45. Thus a number of "big" risks and uncertainties seen on the horizon should be considered methodically, even if there is great uncertainty about their probabilities of occurrence and the impacts were they to occur. These include:

- New laws, regulations or court judgements
- Reactions of hostile interests
- Freaks of nature
- New technologies
- Extreme financial, economic or political circumstances

- Unlikely accidents
- Breaches of contract by third parties
- Failures by suppliers
- Fraud and crime
- Poor internal communications
- Loss of key directors or senior managers
- Risks thought to be unlikely but which would have big impacts.

(This is an indicative list only and is not intended to be complete, nor is every risk on it applicable to every organisation.)

"Warning signs - summary

- Poor internal controls
- Opaque accounting
- Finance function not forward looking enough
- Insufficient focus on cash
- Insufficient focus on shareholder value drivers
- Weak financial structure
- Poor execution of large projects
- Failure to hit sales targets
- Organisational complexity
- Conflict at Board level"

- David Tilston, *Accountancy Magazine*, February 2007

46. An Emerging Risks Report should be prepared for the Board, summarising each risk and its perceived likelihood, explaining its possible direct or indirect impact, stating the arrangements for monitoring it, recommending any responses which should be put in hand before the risk materialises, and setting out ideas on how the risk might be managed after it appears. (A "traffic light system" might be adopted to help the Board to keep track of such risks).

Section 4 – Other important activities of ERM

ERM activities

47. In Section 3 we discussed the management of uncertainty in general terms, and in particular how thinking about uncertainty could influence an organisation's strategic direction. In this Section 4, we describe some of the additional risk-management activities which need to be undertaken as part of an ERM Framework, from an overall corporate perspective, while we reserve to Section 5 the specific actions which need to be taken to manage strategic, project and operational risks.

Risk Appetite and Capacity

48. Identifying the risk appetite and risk capacity of the business is an important starting point for ERM. By "risk appetite" we mean the amount of risk which is judged to be tolerable and by "risk capacity" we mean the extent of the downside risk which the organisation can manage effectively, and bear without getting into serious difficulty if the threats were to materialise, allowing for the possibility that several threats may materialise at much the same time. The following questions may be relevant, among others:

- What balance of risk and reward are we seeking?
- To what extent have we already achieved this balance?
- Would we be prepared to see the business fail completely if extreme events or scenarios arise?
- What are the views of our stakeholders about the extent to which we should take risk? (seeking opinions from shareholders, employees, customers, suppliers, pension scheme trustees, etc.)
- How important is volatility in the business's profits or share price? To what extent (if any) is it important to minimise such volatility?
- Over what period into the future should our risk appetite and risk capacity be assessed?
- How far is our risk appetite and risk capacity a "mathematical" concept, and are non-quantifiable considerations more significant?
- Is there a level of loss beyond which the business could not continue?

- What might cause our customers to abandon us en masse?
- Are there additional sources of cash which we could tap if necessary to remain solvent?
- Is there a difference between our risk appetite and our risk capacity? If so, do we need to change our risk appetite?

Because of the multi-dimensional nature of most businesses, it is likely that there is not a single measure of the risk appetite or risk capacity. There will probably be a series of limits on the risks which can be tolerated, such as:

- A maximum loss of £x in any one year
- A maximum cumulative loss of £y over the next 5 years
- Liquidity benchmarks, including a maximum adverse cash-flow of £p over the next 5 years
- No relaxation of high safety standards for employees and customers
- Go/no-go criteria for corporate transactions (mergers, acquisitions, etc)
- Limits on exposures to derivatives
- Concentration limits for various types of business
- Overall limits on project risk.

Where the total levels of threat in a particular area are deemed to be within the risk appetite and risk capacity, there may be no compelling need to devise responses, but it will often still be advantageous to do so, either in order to achieve risk efficiency or to cover the possibility that several adverse risks might materialise at the same time. Nevertheless most organisations will choose to continue to bear some downside risks which are within their risk capacity, if the cost of avoiding them is too great. The retention of some downside risk is usually essential if business objectives are to have a good chance of achievement, but the *extent* of the risk should be controlled as far as possible.

Scenario analysis and stress testing

49. Useful risk-insights can often be gained by constructing a quantitative theoretical model of a business and then subjecting the model to sensitivity analysis, scenario analysis and stress testing, provided that the business does not fall into the trap of becoming over-reliant on the results produced, which are inevitably restricted by the inability of any mathematical model to represent real life in a comprehensive way. It

will always be necessary for additional scenario and stress-testing analyses to be carried out without invoking the theoretical model, not only to check the results but also to bring a much wider range of considerations to bear. Board members and Senior Executives should appreciate the purpose of the work and the crucially important changes in business strategy which it may indicate are desirable, but they must also understand the limitations of all such attempts to peer into the future and appreciate that any appearance of accuracy is spurious. Actuaries are used to carrying out such assessments in the financial services industry and explaining the results in terms which Boards can understand readily, and it is believed that similar strategic exercises have potentially useful applications in other industries as well.

50. Scenario analysis is the process of considering a limited number of future scenarios and working through their possible consequences for the business. Clearly much will depend on which scenarios are chosen for such in-depth analysis, and ideally they should be based on quite different circumstances which (between them) span much of the future business environment likely to be experienced. The results will probably indicate a wide range of possible threats and opportunities, and lead to suggestions for managing them. However, the method must be supplemented by other ways of trying to forecast possible risks, since it is almost certain that the real-life future experience will differ materially from any of the scenarios selected. (As an example, the details of some possible future energy scenarios up to 2050 which have been developed by Shell, can be found by going to their website www.shell.com, and typing "scenarios" into the search engine.)

51. Stress testing is different in nature. It is solely concerned with downside risk and starts with an analysis of the kind of scenario which could cause the business to fail or suffer serious loss. Stress testing then attempts to analyse how likely such scenarios are to occur and to suggest actions which could reduce the likelihood of occurrence or minimise the impact if they do occur. For example, analysis might suggest that the business could not continue if it were to suffer a loss of more than £100 millions in any one year. Stress analysis would then look at how such a large loss might be incurred, going back as far as possible to the underlying causes which could give rise to it. These would be the underlying threats which would then be explored in depth for possible mitigation. It will be appreciated that such an analysis could be a

complex task, but at least it could identify some of the potentially critical factors. In order to mitigate the possible consequences, it might sometimes be necessary to consider far-reaching suggestions for making the business more robust and flexible, so that it could cope with a variety of future risks, not all of which can be accurately predicted.

Examples of scenarios which could lead to severe problems:

A severe credit crunch
Serious loss of reputation
Adverse legal judgement
Occurrence of adverse event which turns out not to have been insured
Company's products cause health problems for consumers
Sustained interruptions to national electricity supply
Sudden loss of several key executives
Competitor cuts prices suddenly

It is important to avoid an over-mechanistic approach. In the financial services industry, for example, a new solvency capital requirement prescribed by regulators under the Solvency II directive will be calibrated at a 99.5% level of confidence that the firm's assets remain sufficient to meet its liabilities, over a one-year time horizon. However, given the great uncertainties, it is impossible to measure small chances of insolvency accurately, and even if we could, this threshold gives much too great a chance of insolvency (over, say, the first 20 years) to satisfy public expectations. Each organisation will have to devote significant costly effort to the development of sophisticated mathematical models to try to meet this regulatory requirement, but will the effort be worthwhile?

52. The need for scenario analysis, stress testing and indeed the whole approach to enterprise risk which is outlined in this Guide, is underlined by past risk-management experience in the global financial services industry. In 2004-07 many British and US banks adopted aggressive mortgage selling tactics, sometimes even lending as much

as 125% of the market value of the property to people of doubtful credit-worthiness. Many of these risky transactions got packaged up and marketed as though of much better quality to other institutions (often located overseas) who may not necessarily have fully understood the risks embedded in the packages. Very little attention seems to have been paid by senior management to the risk that house prices would decline substantially. When this actually occurred in 2008, many banks and other financial institutions found themselves in great difficulty, which was accentuated by runs on the banks by depositors when the news came out. The need for good ERM practices is underlined by the next box, which gives extracts from an authoritative report on risk-management practices in the industry, dated March 2008, since when the serious problems of some members of the industry have led to bank and insurance failures, extensive shareholder losses and a worldwide recession.

In March 2008 the international regulatory authorities for the financial services industry reported on which risk-management practices worked well in major banking and securities firms and which did not up to the end of 2007: "The predominant source of losses… was the firms' concentrated exposure to securitisations of U.S. subprime mortgage-related credit. In particular, some firms made strategic decisions to retain large exposures to super-senior tranches of collateralised debt obligations that far exceeded the firms' understanding of the risks inherent in such instruments, and failed to take appropriate steps to control or mitigate those risks. Such firms have taken major losses on these holdings, with substantial implications for their earnings performance and capital positions. Another risk management challenge concerned firms' understanding and control over their potential balance sheet and liquidity needs…. Firms that avoided such problems demonstrated a comprehensive approach to viewing firm-wide exposures and risk, sharing quantitative and qualitative information more effectively across the firm and engaging in more effective dialogue across the management team … They had more adaptive (rather than static) risk measurement processes and systems that could rapidly alter underlying assumptions to reflect current circumstances; management also relied on a wide range of risk measures to gather more information and different perspectives on the same risk exposures and

employed more effective stress testing with more use of scenario analysis. In addition, management of better performing firms typically enforced more active controls over the consolidated organisation's balance sheet, liquidity and capital."

- extracts from report of March 6, 2008 from the Senior Supervisors Group to the Bank for International Settlements: *Observations on Risk Management Practices during the Recent Market Turbulence*

Developing responses to risk

53. A crucial part of an ERM Framework is to have appropriate systems in place for developing suitable "value for money" responses to uncertainty. An improved list of responses can usually be developed by the use of imagination and creative thinking. Brainstorming, desk-top research into similar situations, workshops – all have a part to play. It is important not to rely just on the first list of responses identified, but to have standard procedures in place to ensure that this creative thinking process actually occurs. Even for existing well-known risks where responses are already in place, these responses can often be enhanced by creative thinking by people who have not been concerned with devising the current ones.

A pension scheme had safeguards in place to detect frauds by external suppliers of goods and services. At a routine risk review an external risk consultant suggested additional safeguards which could be obtained by using proprietary online databases that were unknown to the manager who owned the risk.

Responses to foreseen threats and opportunities usually take one of two forms - either to change the probability of occurrence of a scenario or event, or to change the impact if the risk materialises. It should be noted that both these are hard to determine accurately, and the degree of accuracy may never be known. For example, it might be thought that the installation of a burglar alarm and prominently displaying it on a property will reduce the risk of burglary, but this can never be known for certain - it

may even increase the true risk of burglary by giving the impression that there is something of value there. There is no such thing as an objective probability which can be used to make decisions. Most probabilities are conditional and understanding the conditions can be crucial - for example, looking at the probabilities of various times it may take to get to the airport by car or train may exclude the possibility that we never get there because of an accident. Because of the difficulties surrounding statements about probabilities, they should often be used with caution when thinking about the true underlying likelihood of occurrence and therefore prioritising a risk for deeper consideration. Similarly, we need to understand whether the assessed impacts if a risk materialises include the knock-on effects or not. Hence determining whether to respond to perceived risks, and how far such responses should go, are inevitably matters of judgement. It may sometimes be possible to visualise responses which reduce undesirable probabilities or impacts at minimum cost, without generating significant adverse secondary risks, in which case it is usually fairly clear that the responses should be adopted. The main issue comes when the cost of proposed responses is significant, and a decision is needed on whether the cost is worth incurring. Account needs to be taken of secondary risks which might arise from a proposed response - for example, if a cleaning liquid is thought to have the risk of proving dangerous in the long term to employees handling it, a possible response might be to change to a different liquid, but if there is only one supplier of the latter, there could be a secondary risk of lack of availability. Despite the difficulties, responding to risk effectively is an essential part of ERM, whether it is reducing threats or increasing opportunities.

54. It is well known that there are several possible ways of responding to threats – reducing the risk by altering the situation (for example by choosing a more reliable supplier), transferring the risk (e.g. by insurance or by outsourcing), pooling it with another party, or taking no action. It is perhaps less well known that there are several similar ways of responding to opportunities – by altering the situation to increase the chance or extent of a favourable outcome (such as increasing the scope of an activity), relaxing constraints, transferring the upside risk to another party which is better able to manage it, pooling the upside risk with another party, or taking no action. Whether looking at threats or at opportunities, it is important to ensure that a methodical but creative and imaginative process is in place to explore all the realistic

possibilities and to arrive at an optimum risk-reward balance. Whenever it is proposed to transfer risk to a third party or to pool risk with them, there is always the possibility that the risk may return if the third party goes out of business, and this point must be carefully considered before going ahead. One useful concept is "risk efficiency", a desirable state which occurs when the threats have been sufficiently mitigated and the opportunities optimised, i.e. a set of responses is found (for a particular area of the business or for the business as a whole) beyond which the marginal cost of introducing an additional response would exceed the utility to the organisation of the resulting threat reduction or opportunity increase. Suppose, for example, that a particular threat could be removed by passing the risk of its occurrence to a third party at a fixed cost which includes a profit margin. The utility of this course of action might be greater to a small company where the risk is significant in relation to its overall finances than it would be to a larger company - so in the smaller company risk efficiency might be achieved by transferring the risk, whereas in the larger company risk efficiency would be achieved by retaining the risk itself.

55. One of the difficulties in responding to risk is that the organisation and/or its stakeholders may have several objectives which conflict to some extent. [See also paragraph 72]. Measurable objectives might relate to cost, revenue or profit, while non-measurable objectives might cover such matters as reputation, trust and integrity. By reducing the risk of one objective being missed, there may be a danger of increasing the risk of another objective being missed - possibly with catastrophic consequences. Such issues need to be discussed at Board level, since it is usually only there that a suitable degree of importance can be attached to each objective, and there may have to be trade offs. An organisation needs to make every effort to understand the objectives of its stakeholders, whether these are stated or unstated. (An example of an unstated objective is that a potential customer usually needs to feel trust in the organisation as well as in its products). One of the most important ways of responding to such risks is to seek ways in which the different objectives may be aligned as far as possible, even if this involves changes to the various parties' objectives or to the organisation's overall business strategy. Discussion with the various parties, or their representatives, may help to achieve greater clarity about the full range of their objectives and where the breaking points might occur. The

problem may well occur in situations where the organisation is working in partnership with other organisations, when the non-alignment of objectives may be hidden at first in the general desire to develop a good spirit of working together, only to emerge in full force when difficulties are encountered at a later stage. Before such partnerships are created the parties need to disclose their objectives fully to each other, and jointly work towards a partnership framework which will be robust in any foreseeable possible scenarios. Where there is to be a formal contract between the parties, they need to make a joint risk analysis and discuss the possible scenarios among themselves at an early stage, rather than just leaving it to the lawyers to produce a contract without the benefit of such a risk analysis.

56. Another of the difficulties in responding to risk is that there may well be pressure to delay implementing the selected response, because it is seen as too complicated, distracting or expensive, or not in accordance with the organisation's present culture. This difficulty should be faced head on, and it may be that some difficult choices have to be made. Any significant deferral of a desirable risk response should be properly authorised, documented and regularly monitored.

Underlying causes of risk

57. In developing responses to risk it is usually necessary to first identify the underlying causes of risk, and then to devise responses to those underlying causes. One of the advantages of a holistic approach to risk is that it should facilitate a study of risks in various parts of the business which have the same underlying causes and may therefore all occur at once in future, possibly with a serious effect on the business as a whole. An example would be where a firm had made arrangements with a number of different customers to supply them with goods and services but there are some specific risks which are common to each contract – perhaps all the contracts could be terminated by the customers at short notice, for example, and this might actually happen if the firm's reputation were to suffer a blow or an economic recession were to develop. Either of these latter scenarios might cause the firm's supply of credit to be cut off at the same time, leading to sudden insolvency. The techniques which may help to identify underlying causes of risk include brainstorming, scenario analysis, concept mapping and pattern recognition [see

Glossary]. Concept mapping is particularly useful for looking at underlying causes of risk, since it requires an analysis of the structure of the business, working backwards from the key objectives to establish which areas of the business may have the most significant influence on whether the objectives are achieved or not. There can then be a stronger focus on the risks in these areas of the business than is needed in other areas. At all levels - strategic, project and operational risks - it is essential to have an integrative understanding of the underlying causes of risk, how far they have been measured, and how far they have not, and how far they are connected with each other, leading to a qualitative framework of risk, with quantitative elements where this is useful.

58. In the case of foreseeable risks, looking at underlying causes is right at the heart of the approach we recommend. For example, the business might consider that there is some risk of an unexpected increase in production costs during the next year, without knowing how serious a risk that is. However, this in itself is not very useful. More detailed analysis might indicate that an increase in production costs could arise from a number of different underlying causes, including an increase in the price of raw materials from abroad, a large pay increase to staff or an adverse legal ruling about the impact of new safety legislation. The risk of a rise in the price of raw materials from abroad in turn depends on some deeper underlying causes, including the risk of higher worldwide demand for the materials, a decline in the value of the home currency, and higher shipping costs. Studying these underlying causes in detail may well increase understanding about the true overall level of risk facing the business, even if many uncertainties remain.

59. Quite often the underlying cause which leads to a business failure may be something which appears at the time to be relatively unimportant, yet it has a number of unforeseen knock-on consequences which bring the business down. This is because a medium or large business is in reality a complex system, in which a disturbance in one section can have widespread interactions. For example, the simultaneous sickness absence of an employee and his/her boss in a food company could lead to a failure to implement normal procedures and hence the issue of sub-standard products which affect customers' health and in turn lead to reputation issues and severe knock-on consequences. If an ERM Framework had been in place, the

reputation risks would have been traced back previously to possible underlying causes and stronger procedures set up, while if the company had had a suitable risk-aware culture, members of the operating staff themselves might have identified the risk and reported it before it occurred.

For want of a nail the shoe was lost.
For want of a shoe the horse was lost.
For want of a horse the rider was lost.
For want of a rider the battle was lost.
For want of the battle the kingdom was lost.
And all for the want of a horseshoe nail.

- old nursery-rhyme

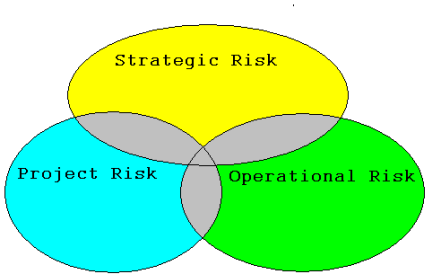
Section 5 – Managing Strategic, Project and Operational Risks

Approaches to risk management

60. In previous Sections of this Guide we have emphasised the importance of studying and managing uncertainty in the widest sense, given the major changes which may well occur in the business and in the world as a whole over short periods of time. These broad considerations must also influence the risk management process throughout the business. Nevertheless, many risks are not completely uncertain, and there will usually be a considerable amount of knowledge about some of them. It is this degree of certainty which enables them to be managed in practice, often very effectively and with a fairly high degree of confidence. In this Section 5 we describe briefly how this risk management should be undertaken, as an integral part of the ERM process. In the interests of clarity we do not continually refer to the need to manage such risks against the background of the previously-described approach to uncertainty in general, but it should be understood throughout that this latter approach must influence the way we proceed, in case we are wrong in thinking we have a high degree of knowledge about the risks concerned, and in order to take account of broader aspects of uncertainty which might upset all our calculations. The risk-response considerations set out in paragraphs 53-59 are also directly relevant throughout this Section.

The three kinds of risk

61. The following diagram illustrates the relationships between the three components of the risks facing an enterprise, namely strategic risk, project risk and operational risk:



The components of Enterprise Risk

Strategic Risk consists of the most important threats and opportunities that an enterprise faces, i.e. the possible future scenarios that would make a material difference (for better or worse) to its ability to achieve its main objectives or even to survive. Often influenced strongly by people's perceptions and behaviour, these risks are composite sources of uncertainty - dynamic and interconnected - and therefore they may need to be managed as complex processes rather than discrete events. Strategic risk includes those project risks and operational risks which could have a material impact on the success of the business as a whole, which is why the diagram shows these three categories as mutually overlapping to some extent. In fact strategic risks often start as project or operational risks, and they may sometimes include risks arising at the point of time in future where project risks will become operational risks. Even if the likelihood that a particular risk will occur is thought to be small, it will still qualify as a strategic risk if its potential impact, were it to occur, might be serious for the business as a whole, bearing in mind that more than one big risk could materialise at about the same time.

Project Risk There is generally a cascade of change projects in organisations - some identified as new, or renewals or upgrades, and some as simply ways of improving operational performance. They may consist of investing in new facilities, launching a new product, or undertaking a business change

initiative. Project risk includes the various opportunities and threats which arise within the projects that the organisation undertakes from time to time. It does not include the risk of whether the right projects are being undertaken or not, which forms a component of strategic risk - however, the work done to appraise the risks on proposed projects can help to manage this aspect of strategic risk successfully. Since at the outset of a project it is necessary to study and respond to the risks throughout the expected lifetime of the project and its consequences, this means that project risk includes the future operational risks arising from the project, until the stage is reached when the project is merged with the main business and becomes managed as "business as usual" - all future risks, including those hitherto regarded as project risks, can thereafter be managed under the heading of operational risks. For example, at the design stage of a new stretch of railway line, the risk of signals being passed at danger ought to be minimised by good design of the track and signal layout, and this is managing a project risk, but once the railway comes into operation the same risk is controlled on a day to day basis as part of the operational risk management process. Hence the diagram above shows project risk and operational risk as overlapping each other to some extent.

Operational Risk consists of the various opportunities and threats which arise routinely in an ongoing business, in fields such as health and safety, fraud, litigation, customer service, staff, suppliers, finance, etc, as well as the risks which arise when the business is changing. Many of these risks are, in principle, common to many businesses, though of course the details will differ. Operational risk excludes the risks which are present in projects, until the stage is reached when a project comes into operation and is merged with the main business. However, there may be some operational risks which arise out of the distraction from normal activities which projects cause before they become operational.

Why have separate categories of risk?

62. It may appear at first sight that these subdivisions of risk are unnecessary, and even confusing because of the overlaps. However, the risks facing large organisations are so numerous and complex that it is essential to break them down

into distinct “chunks” which are manageable by different parts of the organisation. Thus strategic risk needs special attention by the Board. Project risk needs careful consideration from those who authorise the project and from the project managers who implement it. Operational risk, even where it may seem relatively insignificant, needs to be continuously managed by the line managers who are responsible for various aspects of the ongoing business. However, these are not self-contained categories, because of the overlaps, and there does need to be a mechanism to transfer particular risks from one category to another as new situations develop – for example, if a particular operational risk or project risk looks as though it might be starting to assume strategic importance.

How ERM integrates these risks

63. Enterprise risk consists of the totality of the risks which the organisation faces under the three headings, integrating them in such a way as to provide a holistic view of the whole situation. In the process of integration any gaps and overlaps will be remedied. Perhaps the most recent example to which everyone will relate is the extent and suddenness of the global recession - although many good risk analyses in 2007 may well have foreseen an economic downturn as a possibility in 2008, the force with which it actually arrived (including a widespread lack of access to funding) would probably not have been anticipated and it may have been classed as just another operational risk rather than a serious strategic threat. However, if full ERM had been in place, the integration process would have required a study of not only the expected impact if the risk materialised but also the full range of possible scenarios, so the strategic implications if an economic downturn were to turn out to be serious would have been recognised. To take a less dramatic example of how ERM can fill a gap in thinking, consider the case of an organisation which has several large investment projects in the pipeline, that will commence operations in a few years’ time. Although the future operational risks for each project should have been taken into account in the risk analysis undertaken before the project was authorised, it may not be the case that the business has previously considered the full impact on the organisation of the combined operational risks which could emerge when all the projects have commenced operations. These combined risks may not be sufficiently important to be regarded as strategic risks, but there may nevertheless be actions

which could be taken now to manage them more effectively when they start to arise (for example by engaging and training staff). An example of the need for clarity of thought in the process of taking an integrated approach to risk concerns the appraisal of proposed capital projects, where it is common practice for a discount rate to be used to establish the net present value of the project under various possible future scenarios, allowing for risk. If a relatively high discount rate is used, it may already make an allowance for some types of risk, so there is a danger that risk may to some extent be double counted unless care is taken. These examples illustrate the fact that taking an integrated approach to risk requires imagination and clear thinking if a sufficiently wide range of future possibilities is to be considered and if gaps and overlaps in the organisation's standard approaches to risk are to be successfully identified and eliminated. Moreover - and this is crucially important - ERM is not just about the management of an organisation's risks, but it also feeds back the principal conclusions reached about those risks to the overall strategy of the business, which may need to be changed as a result.

> "The essence of 'best practice' in any management context is clarity of thinking and communication, leading to shared appreciation of what matters, appropriate decisions and effective actions, supported by an appropriate integrated approach to concepts, tools, techniques, processes, organisational capability and context."
>
> - *Decisions* (Chapman et al., forthcoming). A copy of the current draft of seven chapters of *Decisions* was made available and drawn upon in several places in this Guide, without adopting some of the more fundamental rethinking of common practice which it recommends. For a published introduction to these ideas, see Chapman and Ward (2003 and 2008).

Managing strategic risk

64. Despite the uncertainties surrounding the business, it is important to realise that some strategic risks are entirely foreseeable. These risks are often capable of being managed in a traditional way, by generating risk responses and then selecting the ones

which seem most appropriate and cost effective. Some examples of foreseeable downside risks are:

- Loss of a key executive
- Failure of a new system
- Serious fraud
- Failed acquisition
- Loss of a major customer
- Unexpected outcome to a major legal case

Examples of foreseeable strategic upside risks might include:

- Successful takeover bid made
- Large contract won
- New product gets big market share
- Difficulties for a major competitor
- Successful rights issue

65. Some examples of strategic risks which are less foreseeable include:

- Chain reactions leading to disasters
- Technological breakthroughs
- Launch of excellent new product by competitor
- Unexpected attacks on reputation

Even though such risks may be more difficult to comprehend and manage, the attempt should always be made, since even a limited insight may be better than no knowledge at all.

> "While only 18 per cent of organisations use board-level discussions and analysis to identify key risks, this approach has become a more common practice than it was in 2007, up from 7 per cent". Aon Global Risk Management Survey, 2009.

66. There may be important risks already embedded in the organisation, for example:

- Existing contracts which might contain unrecognised risks
- Insurance policies, which might not cover as many risks as is currently believed
- Mathematically-based models for controlling financial risks, which might not adequately reflect the extreme events and scenarios of real life
- Key spreadsheets or computer programs which might contain errors that surface only occasionally but with devastating effect
- Inadequacies in the standard methods used for appraising capital projects
- Inadequate control systems, for example on exposure to the more risky types of derivatives
- Lack of training in key operational procedures
- Too much reliance on unproven technologies at the cutting edge
- Lack of sufficient internal governance to prevent the risks which may arise from individuals in the organisation – for example, their lack of skills or experience, or their greed, ambition, demotivation, etc., or doubts about their own responsibilities and accountabilities
- A lack of sufficiently vigorous and timely follow-through from risks which have already been identified in the past.

Such embedded risks should be diligently sought out and studied carefully, and corrective action taken if necessary, being wary of the possibility that actions to reduce a particular risk may increase risk in other directions.

67. One of the key tools for identifying strategic risks is concept mapping. A concept map is a model which allows complex interconnected factors within the business to be shown in a simplified diagrammatic form. Starting with the organisation's objectives, the aim is to identify those areas of the business that could impact on each of those objectives in a significant way. For each identified area, the analyst then works backwards to identify particular issues and activities that could be critical for the achievement of one or more of those objectives. The results are first expressed as a narrative and then plotted on a diagram as a hierarchy of risk areas, which will highlight the areas, and the issues or activities, that could impact

significantly on a number of objectives and where the risks therefore need to be most carefully managed.

68. The effective management of strategic risk requires that a good ERM Framework is in place, as described elsewhere in this Guide, including all the cultural and communication aspects. Because strategic risks are the ones which can make the biggest difference to the organisation, they need to be separately identified for special attention, so that they do not get lost in the multitude of risks which the organisation faces and hence receive insufficient attention. It is often good practice for a short list of (say) the 10 most serious threats and the 10 most promising opportunities to be singled out for regular reviews by the Board itself. Board Members will contribute their own thinking at these reviews, to add to the risk management responses suggested from within the business. From time to time the short lists will change, as new threats and opportunities emerge or assume greater importance, and old ones disappear or become less important (and good horizon scanning will help to ensure that this happens in time). Boards will often appreciate simple graphical presentations (for example, showing the strategic threats and opportunities in the four corners of a likelihood/impact matrix), but this does not absolve them from the responsibility of getting a deep understanding of each of these risks, as well as thinking deeply about the aspects of uncertainty highlighted earlier in this Guide. The actual management of the strategic risks will continue to be entrusted to line managers, under any guidance given to them by the Board, but they will normally be expected to devote more time, effort and resources to the strategic risks than to risks in general.

Managing project risk

69. Detailed guidance for managing project risk is given in the RAMP Handbook. This contains a strategic framework for managing project risk and its financial implications, to increase the chance that the project will prove a success. RAMP is a comprehensive and systematic step-by-step iterative process for identifying, analysing, evaluating and managing project risk, and can be used in conjunction with a suitable investment model to show the range and likelihood of various financial results. (If desired, it can be applied in conjunction with a “gateway system”, where certain defined stages in the evolution of a project have to be completed and

evidenced before going on to the next stage). RAMP covers the entire life of a project, from inception to close-down, and not just the stage before the project comes into operation. One of the main questions which should be asked at the outset is, "What will constitute success?" Very often the answer will fall under two headings:

- Outcomes before operations commence which broadly match current expectations, and
- Stakeholder satisfaction once operation has commenced.

Too often in practice the project manager is focused only on delivering a capital asset within budgeted cost and timescale. While this may be important, it is not the only requirement. It is therefore worth summarising here some key rules for project success, as follows:

Rules for project success

1. Be clear about who is the client, get a full understanding of the relevant objectives of all key stakeholders, and ensure that the project is compatible with those objectives.

2. Define the project's scope, objectives and success criteria thoroughly, after considering all relevant uncertainties about the future. Continually focus on success as the project proceeds, and ensure that there is a high commitment to achieving it.

3. Make the design as flexible as possible, to facilitate operation in a wide variety of circumstances, even if this involves some extra cost. Involve the ultimate users at the design stage and throughout the project.

4. Pay sufficient attention from the outset to the identification and analysis of all significant threats and opportunities, including social and environmental risks, and plan an appropriate set of responses which leads to risk efficiency.

5. Prepare a high-quality appraisal of the project as the basis for a decision on whether to proceed. The appraisal (which will not necessarily be publicised

more widely in this form) should avoid bias and mistakes as far as practicable, highlight the residual risks after the planned responses have been adopted, and present a fair picture of the range and likelihood of possible financial results, and all other relevant considerations. It should include a well-researched and unbiased cost estimate, plus a reasonable contingency allowance for costs which cannot be individually assessed.

6. Establish a good risk-governance system for the project, which avoids excessive organisational complexity, allocates risk ownership, ensures that planned responses to risk are implemented, enables rapid communication between all concerned, and provides for regular risk reviews.

7. Appoint a competent, motivated and empowered project manager, draw up a project execution plan, and ensure that there are sufficient resources to manage and control the project.

8. Develop a comprehensive system of contingency plans (especially where it is proposed to use advanced technology which may prove unsuccessful in this context) and a good system for crisis management.

9. Ensure that there is an effective and well-documented change control process in operation. Establish a point in the project plan beyond which changes in specification will not be accepted, and ensure that all relevant parties agree to this in advance.

10. Ensure that sufficient funding to complete the project is firmly in place, with no likelihood of the funding being withdrawn when the project is only partially completed.

By following these simple rules and applying RAMP, many of the threats to any project will be mitigated and opportunities maximised.

Managing operational risk

70. The management and control of operational risk (both threats and opportunities) is right at the heart of a good ERM Framework. We describe below some of the key controls and approaches which may be found useful, though of course each business is different and will have its own specific risks and controls to add to those mentioned. One important point is that no system of control will entirely eliminate operational threats, so a reserve of spare cash should always be kept accessible to meet unexpected extra costs or shortfalls of revenue. The size of this reserve should be carefully considered, having regard to past experience over at least several years, but it is always prudent to keep an extra reserve on top of this in case new or increased threats emerge.

The nature of operational risk

71. Our research into several major industries has shown that, although between them they have a very diverse set of operational risks, nevertheless the underlying causes of most of these risks can be summarised into 12 distinct categories, as follows:

- Damage to reputation
- Staff issues (including poor administration, failures due to lack of training or knowledge, poor planning for changes, bad communication, labour disputes, management greed, sickness absence, loss of key executives, failure to observe procedures, complacency, corruption, health and safety, etc)
- Problems with IT systems
- Reductions in demand – volume sold, revenues received, competitors cutting prices, new competitors, obsolescence, loss of major customers
- Customer service problems – delays, errors, safety issues, product recall
- Supply issues – poor availability of fuel, electricity, materials, staff, or service from subcontractors, and failures of design or manufacturing
- Third parties – terrorism, fraud, theft, activists, computer viruses
- Fire, explosion, earthquakes, weather
- Legal – regulation, compliance, contracts, damages claims

- Financial – cost increases , cash shortfalls, bad debts, inadequate insurance, interest rate rises, spreadsheet errors, losses on derivatives, pension fund deficits, reduction in profits, decline in share price, extreme events greater than models predict
- Premature deterioration of infrastructure or equipment
- Changes in stakeholder groups or internal organisation

Some of these risks are, of course, linked – in particular, damage to reputation, a reduction in profits or a decline in share price could occur as a result of the occurrence of some of the other risks listed. The important challenge for a business is to set up a system for managing all kinds of operational risk. The best way of doing this will vary from one organisation to another, but there should be a systematic and methodical approach to seeking out and controlling all the various risks which could arise, with particular emphasis on the underlying causes of risk, chain reactions, connections between risks, and the identification of risks which might well occur simultaneously in various parts of the business due to their having the same underlying causes. Where activities are controlled by computer programs, mathematical models or spreadsheets, the limitations of (and the possibility of errors in) those methods must be fully understood and measures put in place to deal with exceptions and extreme events. The risk management process should come to be embedded in all the activities of the organisation in a holistic way - a concept which has been compared to a stick of rock running through the business from top to bottom.

> "Protection against loss [of] and damage to reputation is seen as the most important potential benefit of an ERM strategy" – Economist Intelligence Unit report, *The Bigger Picture*, on an international survey of ERM in financial services organisations, September 2008.

Risk trade-offs

72. As stated in paragraph 55, one of the issues in managing operational risks is that an organisation with several different major objectives might find that a particular risk

response could be beneficial when viewed against one objective and deleterious when viewed against another. For example, there may be conflict between an objective that a company's costs should be kept to a minimum for the next 12 months and another objective that the company's market share should be maintained – the risk of losing a customer who was expensive to service might be seen as positive for the first objective and negative for the second. If such a customer loss was threatened, the management of the business should face up to the issue, and could consider whether there is any "trade off" solution which would enable the customer to be retained but with reduced servicing costs; if not, the conflicting objectives would have to be prioritised. As another example, consider the introduction of speed humps in a city street – it may meet the objective of reducing accidents but could make it more difficult to meet the objective of allowing speedy access for emergency vehicles. It would be desirable to achieve risk efficiency for all the objectives, but this may well be unattainable. Some kind of weighting of the different objectives may be necessary to establish prioritisation rules, but this will often be to some extent arbitrary and the weights may have to change as the organisation comes under pressure from different directions. In recognition of this, risks should often be considered under alternative scenarios with different weight sets. In the rest of this Guide, however, we shall assume for simplicity that this issue does not exist, even though it can often arise in practice and the risk management system must contain appropriate mechanisms for dealing with it.

Reporting occurrences of risk events

73. The first task in bringing risks under control is to construct a reporting system which enables those at the centre of the organisation to become fully aware in a very timely way of all the significant risk events which actually occur from time to time. Many businesses which believe that they successfully manage their operational risks may not have been as successful in this as they think, if they have not had such a system in place. Too often the knowledge of what has occurred is restricted to people whose work brings them close to the event, and its occurrence is not reported more widely. This means that other people cannot learn from the event and how it was managed, which is a waste of a great learning opportunity which might be invaluable to the business in future. Moreover, the risk events which have occurred may well include some which are important pointers to any pressures which are

building up within the business or in its relationships with the outside world, and may therefore help to focus attention on the desirability of strategic changes in the business. Such a reporting system (covering both favourable and unfavourable risk events) is therefore essential to an ERM Framework, and the data recorded on it should include:

- Date and nature of incident, and the consequences of it
- Loss or gain incurred (if any)
- Root causes
- Lessons learned
- Action taken to change the likelihood or impact of similar events in future.

The first two items in this list should be reported promptly and the other three as soon as the relevant details are known. The kinds of incident which should be reported include the following (among others):

- Executives or other staff exceeding the authority which has been delegated to them (even if the result has been positive)
- Breaches of ethical standards
- Failure to operate an established procedure properly
- An IT failure which has had knock-on consequences for business operations
- Serious injury to employees or third parties
- Loss or gain of a major customer
- Damage to the reputation of the business
- Significant fraud, theft or security failures
- Serious manufacturing or distribution failure
- Sudden rise in customer complaints
- Product recalls
- Fire, flood, or explosion
- Adverse or favourable legal or regulatory judgments
- Success of an advertising campaign
- Potentially significant faults discovered in spreadsheets or computer programs.

Definitions will be needed as to what constitutes “significant” or “major” to ensure consistency and to avoid the reporting system being overwhelmed by trivia. It is

important to construct the reporting definitions in such a way as to avoid the system becoming a bureaucratic nightmare - it has to be useful in practice, not too expensive to run, and perceived as focussing on significant issues. There should be a parallel reporting system which deals not with events which have actually occurred but with specific risks which appear to have increased or decreased in importance – for example if system weaknesses are spotted with appear to give rise to increased risks of fraud.

Risk indicators

74. In addition there should be a system of key "risk indicators", which are updated regularly, including standard numerical data on such matters as:

- Customer complaints and commendations
- Staff resignations
- Payment delays by third parties
- Media reports about the business (positive, neutral and negative)
- Production downtime
- Time taken to process customers' orders
- Error rates in processing customers' orders
- IT system availability
- Key financial data

and other risk indicators specific to the individual business.

These risk indicators should be analysed carefully, to see whether there are any indications of a changing trend which needs further enquiries and research.

Review meetings

75. The details of incidents and trends should be reviewed, at least monthly, at a high-level management meeting, preferably one which is attended by both the CEO and a representative of the Central Risk Function. The main aim is to focus on the possibility of new and unexplained trends and the actions which should be taken to respond to them or explore them further (including any indications of pressures building up within the business or in its relationships with the outside world). In addition consideration should be given to the particular responses which were adopted

for the risk events which occurred, and whether alternative action might have been preferable, so that appropriate guidance can be given in case a similar event should occur again. Any areas where risks are seen to have increased recently should receive particular attention, to see if short-term responses need to be adopted. Moreover, it should be considered whether there are lessons for the wider organisation which need to be publicised.

Rapid response teams

76. Consideration could be given to introducing a standard practice whereby, if a particular part of the organisation starts to experience significant adverse operational risk, a cross-functional team will meet promptly with the managers concerned, to offer support, help, and suggestions, but not to allocate blame.

Control cycle techniques

77. One technique which may be helpful for managing certain types of recurring operational risk is to use a repetitious "control cycle" approach based on:

- Modelling expected results
- Measuring actual results
- Seeking good explanations of the difference
- Using these findings to identify the need for additional risk responses and to strengthen the model.

Insurance

78. Insurance can be taken out against many operational risks, and very often in practice the insurance company acts as the catalyst for establishing risk-management processes around the risks insured. It is of course vital to ensure that all the insurer's conditions are met, to avoid the policy being invalidated. However, it may not be worthwhile to take out insurance in all areas, because of the need to pay the insurer's profit margin and expenses, through the premiums charged. One of the advantages of ERM is that it considers risk holistically and can therefore identify those operational risks which are relatively small in the context of the overall risk which the business faces and hence no longer need to be insured, thus saving some money even after allowing for the cost of meeting the claims direct. (More information regarding

companies' insurance arrangements is given in the Aon Global Risk Management Survey 2009).

Fraud

79. Fraud is an operational risk which is unfortunately becoming more prevalent and, at its worst, could cause an organisation to go out of business. For fraud by employees, insurance broker Marsh has recommended the preventative measures set out in the box.

- Vigilance – look out for increasing levels of employee stress or out-of-character behaviour patterns
- Controls: ensure segregation of duties in high risk areas; enforce holidays and the handover of work
- CV check: if hiring new staff, take up references and check qualifications
- Security: ensure that exit procedures are robust and that both physical access to premises and computer access are appropriately limited or removed
- Staff 'buy-in': ensure that a comprehensive whistle-blowing policy is in place; encourage staff to raise concerns about malpractice and create an open working environment

Source: Report in *The Actuary*, Jan/Feb 2009

Other ways of combating fraud include a brainstorming process to identify areas of vulnerability where further study is necessary and improved precautions may be required. Audit processes may also need to be strengthened.

Risks associated with change

80. When changes in the business pattern or the organisation of the business occur, this is usually associated with extra risks, which may not be fully recognised. It may well be necessary to supplement normal risk controls at a time when the organisation is in the process of change or is developing new activities, the aim of the additional controls being to detect the emergence of new risks or perhaps a rise in ordinary risk levels due to management taking their eye off the ball due to the distraction of the changes. If a management position will cease to exist as a result of organisational

changes, any risk control functions associated with the post or its present occupant must be carefully identified and transferred to one of the remaining management positions. Failure to do this is not uncommon and can result in some unpleasant surprises.

81. One kind of change which often arises in practice is a decision to increase market share or at least to stem a declining trend in market share, by adopting more aggressive sales tactics. This very often involves the taking of extra risks, such as customer dissatisfaction, inability to fulfil the extra orders, or retaliation from competitors. The need to increase sales may sometimes be considered so urgent that time-consuming mitigation actions for the extra risks may be brushed aside. The governance system in all companies practising ERM should ensure that such risks are not disregarded but are properly aired and debated at an appropriate senior level.

82. When a business decides to diversify in order to become more robust or to grow more rapidly, it may be tempted to pursue a course of acquisition or merger in order to make the change become effective earlier than could be done otherwise. This is not the place to discuss the pros and cons of such a course, other than to observe that a large percentage of mergers and acquisitions seem to fail to achieve their objectives, and often the reason is either because too much is paid at the outset or because of a clash of cultures which cannot easily be resolved.

> A large international company proposed to acquire a small but profitable German company which had a complementary product range in one area and about 20 employees. Due diligence confirmed profitability and the acquisition looked as though it would go ahead. At the last minute, someone asked whether there were any pension risks. It transpired that the three founders were about to retire with contractual entitlements to pensions, but no cash had been put aside for this. Instead of buying an ongoing business, the international company would have bought a pensions liability!

83. An ERM Framework therefore needs to incorporate procedures which alert the Central Risk Function at a very early stage when major change programmes are being developed, so that the best possible risk analysis in the time available can be carried out and taken into account in the decision on whether to proceed.

Contract bidding risks

84. There are clear downside risks for the organisation when the team bidding for a major contract:

- has insufficient knowledge about all the factors involved, or
- has not enough experience of past contracts and the adverse events which occurred, or
- is incentivised to "get the contract at any price".

Carefully designed governance procedures are necessary to ensure that such risks are kept to a minimum, though sometimes it may be possible for some of the risks to be managed by the inclusion of appropriate flexibility clauses in the contract.

Crisis management

85. It is also important to have a fully adequate mechanism for managing unexpected situations at short notice. Sometimes an organisation will fail because of an inadequate or destructive response to a situation, rather than because of the situation itself.

> It was not the Enron crisis itself which led to disaster for its accountants, Arthur Andersen, but the latter's response to the crisis, which destroyed the confidence of its other clients. If Arthur Andersen's internal culture or crisis-management machinery had been different, they might have been able to remain in business.

Under-reaction should, of course, be avoided as much as over-reaction. The most careful consideration should therefore be given to the nature of the crisis management mechanism and who should participate. Adequate contingency plans should be prepared in advance – these should include not only some comprehensive business

continuity plans for dealing with physical disasters and major IT problems, but also plans for dealing with threats to reputation.

> "Enterprise-wide disaster recovery plans are in place at just 35 per cent of the companies". RSM McGladrey 2009 Manufacturing and Wholesale Distribution Survey, based on replies from 920 executives in the USA.

The group of people concerned in crisis management should be empowered to take entirely unprecedented or unforeseen action speedily if necessary, but with safeguards as far as possible to prevent the group from over reacting due to the pressures of the moment.

> Railtrack's sudden imposition of drastic speed restrictions right across the network after the Hatfield accident may have contributed to its demise, whereas a more measured response might have enabled it to survive.

Section 6 – Risk Governance

Why risk governance matters

86. In practice it has sometimes been the case that the principal reason for the failure of an organisation can be traced back to the failure to have a proper system of risk governance in place. Even very large organisations have fallen into this trap, for example by combining key senior positions which should have been occupied by separate people who could place a check on each other. (The Equitable Life Assurance Society in the UK is one example where this occurred and it was later identified as one of the reasons for the difficulties which the company experienced). It is still the case today in a few companies that the posts of chairman and chief executive are combined, despite shareholder pressure to outlaw the practice. Good risk governance is crucial to ensuring that the systems which have been introduced to control risk are adequate and are being operated properly.

Controlling staff risks

87. Since staff are one of the greatest sources of downside risk to an organisation, there must be an appropriate system in place to minimise these risks. Every reader will know of cases where an organisation has been brought down by the excessive risks taken by an unsuitable occupant of the post of CEO or CFO. Often the risks are taken in the interests of sales growth, or as the result of alleged pressure from the City, without sufficient regard to what may go wrong. Sometimes an apparent new opportunity is created by a legislative change, and the organisation is led by senior management into unknown territory without sufficient thought.

> When the law was changed in 1988 to prohibit organisations from making membership of their pension scheme compulsory, which had been the norm up to that time, many life assurance companies saw an opportunity for new business. Their salesmen, untrained in relevant skills and eager for commission, persuaded many existing pension scheme members to leave the scheme and take out an individual pensions insurance policy instead, even though it was clearly not in their interests to do so. The resulting mis-selling

scandal, which took some years to emerge fully, resulted in a severe loss of reputation for the life companies concerned. This affected their ability to generate future new business due to a loss of consumer confidence, and they were also required to undertake a very expensive rectification exercise for the individuals who had suffered.

The most important aspect of risk governance is therefore to ensure that the people leading the organisation have a responsible attitude to risk, including sound professional ethics. They should also be people who understand ERM fully and who can appreciate the importance of the issues outlined in this Guide. Their remuneration structure should be designed to reward them for the organisation's success in the medium term, and not just in the current year. The organisation's leaders should also ensure that suitably responsible people are chosen to fill management posts and should provide them with appropriate training in ERM issues, as well as ensuring that their remuneration structure is properly aligned with the degree of risk which they should be taking and the period over which their performance should be judged from an ERM viewpoint.

System of checks and balances

88. It is important to establish a system of checks and balances to prevent any individual from taking excessive risks on behalf of the organisation. Each person (even the CEO) should be made fully aware of the limits of his or her authority and there should be a comprehensive monitoring system. If someone does exceed his or her authority (even if the result turns out to be positive), this should be regarded very seriously and lead to disciplinary proceedings. Of course, situations may arise in practice where it is desirable for an individual's predetermined limit of authority to be exceeded, and there must be a simple mechanism, involving at least one other person, to enable this to happen without delay where appropriate. When that mechanism is invoked, those giving the additional authority should sign some appropriate documentation.

Processes and procedures

89. It is essential to put in place appropriate processes and procedures to ensure there is adequate monitoring of changes in the risk profile, to gain positive assurance about the extent to which all risks are being properly managed, to monitor how the ERM system is improving, and to identify further actions which may be desirable. The following actions are necessary:

a. Procedures must be introduced to review periodically the risks which have been identified and the extent to which the agreed risk responses have been actually implemented.
b. Other procedures should be put in place throughout the organisation to ensure that higher management, and the Board if necessary, are notified promptly of significant changes in risk exposure or of any concerns expressed by regulatory authorities.
c. All managers should be required to report at least annually, as a matter of routine, on the risks in areas for which they are responsible, and the actions they have taken to respond to the risks or control them.
d. Project managers in particular should be required to report regularly on the projects for which they are responsible, including any significant concerns they may have developed about future risks once the project becomes operational.
e. Since it is vital that risk management has the support of the CEO, consideration should be given to adding suitable responsibilities into his or her job description and reward criteria, requiring promotion of an ERM framework and culture, and the provision of regular information and assurances to the Board about opportunities as well as threats.
f. A system needs to be in place to analyse the organisation's failures and successes as a matter of course and ensure that the lessons from them are distributed to staff who could learn from them.

All these processes, procedures and systems need to be embedded as far as possible into the ordinary day-to-day management of the organisation.

Key Governance Questions

Leadership – do senior management support and promote risk management?
Are there sufficient checks and balances at the senior level?
Is there enough thinking about uncertainty in general and its implications?
Is the approach to risk sufficiently holistic?
Are staff equipped and supported to manage risk well?
Is there a clear risk strategy and risk policies?
Is there a risk-aware culture and good internal communication on risk?
Are there effective arrangements for managing risks with partners?
Do the organisation's processes incorporate effective risk management?
Does risk management contribute to achieving outcomes?

Adapted from *Risk Management Assessment Framework*, HM Treasury, 29 Ocober 2004

Audit of the risk-management process

90. There needs to be an annual independent audit of the risk management process itself, which could well be carried out by the organisation's internal audit department. The results of the audit must be reported to the Board, and should cover such matters as:

- The progress which has been made towards achieving a suitable risk-aware culture and communications system throughout the business
- Progress on the risk training of managers and other staff
- The effectiveness of risk-related communication with suppliers and customers
- The documentation of risks and responses, including evidences
- The effectiveness of reporting systems - risk occurrences, risk indicators, data accuracy, etc
- The extent to which the Central Risk Function has discharged its tasks
- Regulatory compliance
- The effectiveness of the mechanism for categorising certain risks as strategic, so that they receive special attention
- The amount of time which the Board itself has devoted to ERM

- Progress on the action plan for eventual full implementation of ERM
- Priorities for improvement.

The challenge is to undertake these audit activities in a constructive way which prevents the development of a box-ticking mentality throughout the organisation.

Board risk committees

91. In order to enable more board-level time to be devoted to ERM, some Boards establish Risk Committees made up largely of selected Board members. In such cases it is still important that the main Board is regularly given a sufficient overview of the situation. We do not recommend that the Board's Audit Committee should be given the role of Risk Committee in addition to its audit role, as the audit and ERM functions are very different from each other and must not be confused - as indicated above, internal audit has a crucial role to play in monitoring the risk-management process, while ERM demands an entirely different kind of approach, of a more creative and strategic nature.

Parents and subsidiaries

92. In those cases where the organisation has a parent body, there is a need to ensure that there is adequate two-way discussion with the parent on all risk-related matters, and similarly a parent must ensure that it fully understands all the important risks which may arise in its subsidiaries. It would clearly be helpful if parents could ensure that the same risk language is used by all their subsidiaries (see paragraph 15), and that there is a consistent data flow and a consistent reporting system on risks.

We interviewed a senior executive of a large construction company which was run as five separate business units, using a decentralised approach driven very much by financial performance, and leaving each unit to manage its own risks. The returns earned by all five units started to deteriorate but initially the only action taken at the company's centre was to tell the businesses that they must improve. It was some time before messages began to filter back about the nature of the problems each unit was experiencing, and it was only then realised that there was a common underlying cause which had resulted in them

all losing market share, namely the introduction by a competitor of a new concept which met customers' needs. If this had been apparent earlier, through a good system of communication about emerging risks, a similar change in the company's own services would probably have sufficed, but now the only option was to fight back by reducing prices, even at the cost of lower profits.

Section 7 – Developing an action plan

What kind of action plan is necessary?

93. In this Section we outline in principle the main steps which are necessary to develop and implement an action plan to introduce an ERM Framework. We shall assume here that we are dealing with a fairly complex large or medium-size organisation, where comprehensive systems and procedures are essential in order to endure that all members of staff play their part efficiently. In smaller or less complex organisations not all of these steps may be necessary and it may be possible to implement in a simpler way an ERM Framework that is sufficient for their purposes - though it would still be vital to ensure that the most important requirements are met in one way or another. In either case it will usually be desirable to graft the action plan on to the existing risk-management practices in the organisation, many of which can probably remain in place with only limited alteration, rather than starting again with a clean sheet of paper.

Preparing to implement ERM

94. Like any major project involving a journey over a number of years, the Action Plan needs to be realistic in its goals, sub-goals and timescales. Some of the key tasks preceding it will be as follows:

Study existing risk practices

- Do a quick self-assessment check (such as that appended to this Guide)
- Carry out a comprehensive survey of existing risk practices
- Ascertain which parts of the organisation and which risk practices are priorities for improvement in risk management

Construct a vision of future risk management

- Develop a vision of how the organisation will look different once ERM has been introduced, including an evaluation of the benefits it will bring

- Determine what changes are needed to achieve the vision, including any changes necessary to improve the quality or timeliness of the flow of data within the organisation

Plan the implementation and seek authorisation

- Set out in detail the steps which will need to be taken in order to achieve these changes - some of the possible steps which may be needed are set out in paragraph 95
- Decide the timescale for setting up a Central Risk Function (or strengthening the existing one) and determine its remit and reporting lines
- Determine the timescales for other parts of the Plan and who will be responsible for achieving them, with clear milestones along the way
- Determine how everyone is to be trained to new ways of thinking, behaving and communicating, and make realistic estimates of how long this is likely to take and how much it will cost
- Make realistic estimates of the costs of the implementation project
- Identify the risks of the implementation project and use a recognised methodology such as RAMP to appraise and control them
- Have regard to the rules for project success set out in paragraph 69

Seek authorisation and prepare to get started

- Ensure that the implementation project has full buy-in from the Board and the CEO
- Appoint suitably skilled senior people to lead the implementation process, including a project manager
- Set up a governance structure for the implementation project.

Constituents of an action plan

95. This paragraph sets out some of the steps which may need to be included in the plan for the implementation project outlined in paragraph 94. Much will depend on

how far the organisation has already developed at least some of the requirements, and which are considered the most urgent matters to tackle first. It is important to ensure that the ERM Framework is kept fairly simple and is not "over- engineered", so that all employees can fully understand it and its purposes. It would be a mistake to try and implement it faster than the organisation can absorb it, bearing in mind the need to carry on "business as usual" during the implementation period. A series of short steps may well be preferable to a "big bang". The necessary steps may include some or all of the following:

<u>The Board itself</u>

- Widen the Board's experience if needed, by appointing non-executive directors from outside the industry
- Ensure that all Board members are fully briefed on ERM concepts
- Allocate regular time at Board meetings for ERM and the supervision of the principal strategic risks

<u>Organisational matters</u>

- Introduce whatever changes are necessary in culture and communications [paragraphs 13-18] - these changes may be significant and time-consuming
- Set up a Central Risk Function (or strengthen an existing one), appoint a leader, decide on its remit, and get it to start the tasks outlined in paragraph 21.
- Adjust the organisational structure so that it facilitates the input of the ERM conclusions to the corporate strategy and business development departments, with a view to making the business more robust and flexible [see paragraphs 40-46]

<u>Improve the methods used for managing risks</u>

- Set up systems for developing appropriate responses to risks, using a methodical but imaginative and creative approach
- Establish monitoring systems for focusing on specific risks for which no adequate response has been implemented
- Review, and improve where necessary, the various methods used for managing strategic, project and operational risks [see Section5]

- Establish criteria for determining when project risks and operational risks become sufficiently important to be regarded as strategic risks which could have a significant impact on the business as a whole.
- Study risks which are already embedded in the organisation [see paragraph 66]

Reporting systems

- Improve reporting systems, so that up-to-date and consistent data is available to all those who control risks – many firms in the financial services area are finding this hard to achieve [see paragraphs 73-74]
- Introduce horizon scanning for emerging risks [see paragraphs 44-46]

Risk Governance

- Clarify the responsibilities and ownerships of all managers on risk issues
- Overhaul risk governance systems and ensuring that they are properly developed and implemented, along the lines set out in Section 6.

Procedures

- Start the process of embedding risk-management within the general management of the organisation, so that it becomes part of every manager's way of life – this is one of the hardest things to achieve in practice, since many managers habitually push risk management to the back seat when urgent decisions have to be made
- Ensure that procedures are in place to subject all major change initiatives to risk analysis before deciding to proceed [see paragraphs 80-83]
- Set up a crisis management system [paragraph 85]
- Have better and more frequent discussions with suppliers and customers about emerging risks

> "The end goal for those implementing ERM is to create greater awareness of risk and reward tradeoffs, and to drive risk thinking and appropriate risk management throughout the business" – *The Risky Business,* The Conference Board, 2007

Implementing the plan

96. Implementing such a major programme of management change will, of course, involve significant risks. Managing change is an art in itself, and leadership from the top is essential, as is close monitoring of the implementation process. Since some of the key risks relate to staff perceptions, it is suggested that staff representatives should be consulted over the design of the more important changes and in the reviews of progress, and that surveys should be carried out regularly to test employee opinions. In some countries such consultation procedures will be embedded in local laws.
The threats to the implementation project include cost escalation, lengthening timescales, distraction from the business, a developing lack of conviction about the value of ERM, and accusations of having created a costly and unnecessary bureaucracy. On the other hand, the objective is to achieve proactive confident risk-management, and the opportunities include better credit ratings, identification of profitable new business activities, more rapid responses to new risks, increased motivation of staff from having their inputs respected, a greater confidence in the organisation's long-term future, and eventually a higher share price or (in the case of the public sector) a more sustainable and efficient service for the community as a whole.

Section 8 – Conclusion

Obstacles to the introduction of ERM

97. It will be apparent that it is not an easy task to set up an ERM Framework of the kind described in this Guide, covering all kinds of enterprise risk in a holistic way, and it is not surprising that many businesses are finding it difficult to achieve successfully. Sometimes the cultural and internal communications aspects are given insufficient attention, with only lip service being paid to them, rather than the intensive staff training programme which may be needed. The underlying causes of risk may not be sufficiently explored. Uncertainties incapable of measurement may be largely ignored. There may be only an inadequate attempt to integrate the various kinds of risk and explore the relationships between them systematically. Sometimes the strategic risks are not sufficiently distinguished from the multitude of risks which the organisation faces, and as a result there is insufficient focus on them. There may be insufficient follow-through after risk identification, so that threats remain unmitigated and opportunities unexploited. Sometimes the organisation is dominated by a leader who mistakenly believes that his or her own experience is sufficiently wide to manage whatever situations may arise, and regards risk management as being merely a box-ticking exercise designed to secure a satisfactory credit rating or to satisfy regulatory authorities. Perhaps a risk manager is appointed who is not well versed in ERM techniques – or one who does not have sufficient stature within the company to be able to challenge established practices which appear to carry undue risk, or one who has come from another department whose own practices he should now be challenging. The crisis management system may be inadequate, with few contingency plans and a lack of clarity about the extent of the crisis management committee's authority. Often the Board does not devote enough time to risk management, even though it is arguably one of their most important functions.

The end goal

98. We hope that this Guide will help you to overcome such issues by enabling you to construct your own ERM Framework and increase your chances of success. Our belief is that your business will ultimately be much stronger and more resilient, and people in the business will have greater confidence that it is being well managed, with

the opportunity for everyone to play a part. We have emphasised the fact that ERM demands constructive and imaginative forward thinking, and we firmly believe that a business to which such thinking has been applied will have a much greater chance of ultimate success than one where the risks are not fully understood and the quality of thinking about the future is relatively poor. The former will have a better chance of avoiding disasters and a better chance of identifying and exploiting opportunities in a properly risk-controlled way. The transition from the present risk-management processes may not be an easy one, but we suspect that, in 25 years' time, many of today's businesses which have fallen by the wayside will not have made the effort - while many of the survivors will have a full and active ERM Framework in place, functioning effectively and embracing the cultural changes necessary for it to thrive as it should.

99. If you are still not convinced that you need to adopt ERM in your organisation, why not try answering the simple self-assessment check in Appendix 1?

Glossary

Brainstorming: An intense and focused but spontaneous scrutiny of an issue by a group of people led by a facilitator, to encourage people to put forward relevant ideas.

Downside Risk: See Risk

Central Risk Function: One or more managers at the heart of the organisation who are specifically charged with a number of responsibilities relating to risk, but who are not normally responsible for the process of actually managing risks. [See paragraphs 20-21.]

Compliance: See Regulatory Compliance

Concept Map: A model which allows complex interconnected factors to be shown in a simplified diagrammatic form, so that the overall picture and the linkages can be understood and communicated to a wider audience [see paragraph 67.] [For an example of a concept map, please see page 23 of the STRATrisk Guide, which also gives additional guidance on its use in the management of strategic risks].

Downside Risk: Exposure to unfavourable outcomes

ERM: Enterprise Risk Management. The ongoing proactive process of adopting a holistic approach across the enterprise to all the uncertainty which may affect either positively or negatively the achievement of its key purposes and objectives, leading to action to achieve greater business robustness and flexibility, efficient risk-taking and an appropriate risk-reward balance. [We regard this definition as superseding that given by COSO (Committee of Sponsoring Organisations of the Treadway Commission) in September 2004, which is of more limited application].

ERM Framework: A set of processes which will enable ERM to be implemented effectively within an organisation.

Event: See Risk Event

Flexibility: The extent to which an organisation can rapidly modify its activities in order to meet changing circumstances.

Fuzziness: One kind of uncertainty, where there is a degree of knowledge about the likelihood or impact of an event or scenario but the knowledge is imprecise.

Governance: See Risk Governance

Impact: The range of effects on the organisation if a particular event or scenario materialises. It may sometimes be possible to summarise these effects in financial or numerical terms, but in other cases the impact will be capable of only a qualitative description or even be wholly or partially unknown.

Likelihood: The chance that a particular event or scenario will materialise. Sometimes there may be a degree of knowledge about the order of magnitude of the likelihood, but this is not always the case. Estimates of likelihood may occasionally be quite wrong, due to the existence of underlying causes of which we are unaware.

Mitigation: Action taken to reduce either the likelihood or impact of a threat.

Models: Attempts to represent key features of a business, or the business as a whole, by quantitative processes designed to explore the future progress of the business, allowing for risks and their likelihoods and impacts. The use of such models must not be allowed to obscure awareness of their limitations and possible pitfalls. Models should always be tested by applying sensitivity analysis to key numerical parameters in them or even to the structure of the model itself.

Operational Risk: The opportunities and threats which arise from the operation of the ongoing business. [See paragraphs 70-85.]

Opportunities: Those components of uncertainty which may give rise to favourable outcomes.

Outcomes: The results, events or scenarios that may actually occur at a future point of time, or over a future period. Outcomes may be divided into unfavourable, expected or favourable categories, according to present perceptions (which may change in future).

Overall Risk: The totality of all the downside risks facing the organisation.

Pattern recognition: The process of turning a jumble of disconnected information into trends which may be significant [see page 24 of the STRATrisk Guide].

Positive Assurance: A process of regularly reviewing risk management throughout the organisation, which enables reports to be made to the Board about the extent to which all the risks are being properly managed.

Project: Any organised business activity designed to bring about change, where there is a period of time during which part of the activity takes place before the change becomes operational. Projects may well involve the investment of money and resources. They often consist of the creation of a real or tangible asset, for example in the construction of a building or a piece of machinery, which will generate a flow of goods and services to be consumed in the future. Sometimes, however, they do not involve the creation of such an asset, for example in the launch of a new product manufactured by existing assets, or in a major reorganisation of the business. A project needs to be considered over the whole lifetime of the activity, though in practice there usually comes a point of time when the project becomes (or is about to become) operational and its management is then merged with the management of the main business. When that point of time arrives, the project's risks cease to be managed as Project Risk and start to be managed as Operational Risk.

Project Risk: The opportunities and threats which arise within the projects that the organisation is undertaking to bring about change but which have not yet become operational, including the operational risks which will arise in future once the project becomes operational and merges into the ongoing business. [See paragraphs 61 and 69.]

RAMP: A recognised methodology for analysing and managing Project Risk [see paragraph 69 and the first item of "selected further reading" at the end of this Guide].

Regulatory Compliance: the extent to which all the activities of the organisation comply with relevant laws and regulations (bearing in mind that there may be penalties for breaches).

Response: See Risk Response

Risk: Normally means the same as downside risk. However, where the context requires (e.g. when speaking of risk management or risk efficiency), we sometimes use the word "risk" to cover favourable as well as unfavourable outcomes.

Risk Appetite: The extent of the downside risk judged to be tolerable in each area of the business or in the business as a whole.

Risk Capacity: The extent of the downside risks which the organisation can manage effectively, and bear without getting into serious difficulty if the risks were to materialise, allowing for the possibility that several risks may materialise at much the same time. Risk Capacity may differ from Risk Appetite.

Risk Efficiency: A desirable state which occurs when the threats have been sufficiently mitigated and the opportunities optimised, i.e. a set of risk responses is found, beyond which the marginal cost of introducing any additional response would exceed the utility to the organisation of the resulting opportunity increase or threat reduction. Unlike the Risk-Reward Balance, Risk Efficiency can relate to particular segments of the business or to particular projects. (A graphical approach to risk efficiency and the role of component sources of uncertainty, first used at board level by BP in the 1970s, may help in understanding alternative proposed uncertain choices, as outlined in Chapman and Ward (2003 and 2008).

Risk Event: A definable specific occurrence (either favourable or unfavourable) which may suddenly happen in future.

Risk Governance: A system which establishes and maintains suitable risk-management standards and procedures within the organisation. It also monitors compliance with those standards and procedures, as well as the effectiveness of the whole risk-management process. [See Section 6.]

Risk Indicators: Standard data which are regularly updated and examined for evidence of changing trends which need further enquiries and research. [See paragraph 74.]

Risk Management: The process of identifying, analysing and suitably responding to both upside and downside risk.

Risk Policies: The policies adopted by the organisation in order to manage and control its risks.

Risk Responses: Actions taken to improve opportunities or mitigations to reduce threats. [See paragraphs 53-56, and Section 5.]

Risks (in the plural): Unfavourable outcomes.

Risk-Reward Balance: A desirable state where the overall risk is thought to be commensurate with the possible rewards – generally, the greater the threats, the greater should be the possible rewards. Two necessary conditions for the achievement of a sustainable risk-reward balance are, firstly, that an investor could not achieve a greater expected reward elsewhere for the same level of risk, and secondly that any change in the organisation's policy which would give rise to extra expected rewards would also give rise to additional risks that are judged to outweigh the benefit. Whether an organisation has achieved a risk-reward balance will often largely be determined by comparison with the risks and possible rewards available outside the organisation, though such comparisons are usually difficult because of the difficulties of measurement. In the case of quoted companies the share price will normally find a level where there is a risk-reward balance from the viewpoint of new investors, so such companies may need to consider whether any proposed changes of

strategy will affect the market's perceptions of the risk-reward balance in a positive or negative way.

Robustness: The state where vulnerability to downside risk is as low as possible.

Scenario: A hypothetical situation in the future. The analysis of a scenario does not necessarily need to take into account the likelihood of its occurrence, and sometimes a complete absence of probabilistic thinking is useful. Whatever key events or situations are envisaged in the scenario, its analysis should take account of possible knock-on effects, both positive and negative. [See paragraphs 49-52.]

Secondary risks: New threats and opportunities which arise as a result of the responses adopted to other risks. They can sometimes be important and need to be analysed in their own right.

Sensitivity Analysis: A technique used to discover how sensitive the results obtained from models of the business are to changes in the input values of the variables used to construct the models or to calculate the results. A high degree of sensitivity is a warning to interpret the results of the model with care and circumspection, especially because many of the input variables will themselves have been estimated and therefore subject to error. Even the model itself may be subjected to sensitivity analysis, by exploring the effects of altering the model's structure.

Stakeholders: Those parties whose interests may be affected positively or negatively by the organisation and its activities. For example, stakeholders may include some or all of the following: shareholders, bondholders, banks, suppliers, customers, staff, pension fund trustees, business partners, or the community as a whole.

Strategic Risk: The most important risks and uncertainties facing the organisation, i.e. the possible events or future scenarios that would make a material difference (for better or worse) to its ability to achieve its main objectives or even to survive. Strategic risk may include some parts of Project Risk and Operational Risk. [See paragraphs 61 and 64-68.]

STRATrisk: a process for managing Strategic Risk [see the second item of "selected further reading" at the end of this Guide].

Stress Testing: The process of examining the downside risks which would cause serious difficulties or even complete failure for the organisation. [See paragraph 51.]

Threats: Those components of uncertainty which may give rise to unfavourable outcomes

Uncertainty: Incompleteness of knowledge, i.e. a shortfall of knowledge or information about:

- what kinds of outcome may occur,
- the factors which may influence future outcomes,
- the extent to which known and unknown factors will influence outcomes,
- the likelihood or impact of various outcomes.

Some uncertainties may not even be seen at all, while others may involve fuzziness. Different people may perceive different degrees of uncertainty, according to their knowledge and experience. Some people find it helpful to think of uncertainty simply as "lack of certainty" in the widest sense. [See Section 3.]

Upside risk: Exposure to favourable outcomes.

Variability: All the variations in outcomes which can occur, whether downside, expected or upside.

Vulnerability: The extent to which the organisation may be affected by adverse impacts if risks materialise.

Selected further reading

- Actuarial Profession and the Institution of Civil Engineers. *RAMP - Risk Analysis and Management for Projects (second edition).* Thomas Telford, 2005.
- Actuarial Profession and the Institution of Civil Engineers. *Strategic Risk - a Guide for Directors.* Thomas Telford, 2006. This Guide is known colloquially as STRATrisk.
- Aon *Global Risk Management Survey*, 2009.
- Chapman, Chris B. and Ward, Stephen C. *Project Risk Management, Second Edition*, Wiley, 2003.
- Chapman, Chris B. and Ward, Stephen C. Developing and implementing a balanced incentive and risk sharing contract, *Construction Management and Economics, Volume 26,* Numbers 4-6, pages 659-669, 2008.
- Chapman, Robert J. *Simple Tools and Techniques for Enterprise Risk Management*, Wiley, 2006.
- Economist Intelligence Unit. *The Bigger Picture – Enterprise risk management in financial services organisations.* September 2008.
- Halpert, Aaron M. and Marlo, Leslie R. *Linkage of Risk Management, Capital Management, and Financial Management* [Joint CAS-CIA-SOA Risk Management Section White Paper Project, May 2007].
- Hexter, Ellen S. *Risky Business – Is Enterprise Risk Management Losing Ground?* The Conference Board, 2007.
- HM Treasury. *The Orange Book. Management of Risk – Principles and Concepts.* October 2004.
- HM Treasury. *Risk Management Assessment Framework – a Tool for Departments.* 29 October 2004.
- International Actuarial Association. *Practice Note on Enterprise Risk Management for Capital and Solvency Purposes in the Insurance Industry.* August, 2008.
- Lam, James. *Enterprise Risk Management, From Incentives to Controls.* Wiley, 2003.

- Tilston, David. *Warning Signs*, article in Accountancy magazine, February 2007.
- Tripp, M.H. et al. *Quantifying Operational Risk in General Insurance Companies*, 2004, British Actuarial Journal, **10**, V, 919-1026.

Appendix 1

ERM self-assessment check

Mark out of 10
(10 = excellent)

1. Does your organisation think deeply and broadly enough about uncertainty and take steps to manage it proactively and systematically?
2. Is your organisation using the results of holistic analyses of uncertainty to influence strategy and business development?
3. Are you sure that all the most significant threats and opportunities facing your organisation are being managed effectively?
4. Are you confident that your business is likely to survive major external changes in future?
5. Does the Board make enough time for understanding risk?
6. Does it give good risk-leadership to the organisation?
7. Do you have an effective central risk function which attempts to "see the whole picture of risk"?
8. Is there an adequate system for spotting emerging threats and opportunities in time?
9. Is there clear and regular communication on risks throughout the organisation (up, down and sideways) within an appropriate risk-aware culture covering both threats and opportunities?
10. Is your system of risk governance good enough?

If you have scored less than, say, 75 out of 100, we suggest you may wish to think seriously about moving further in the direction of ERM.

Appendix 2

ERM Group members

Simon Adams, Chartered Civil Engineer and member of the Association for Project Management. Simon is Head of Business Planning for Crossrail Ltd and responsible for overseeing the application of risk management to that enterprise. His recent career has specialised in understanding the uncertainty associated with long-term investment programmes, with practical experience of the application of StratRisk and Ramp.

Neil Allan, civil engineer, visiting lecturer in Construction Management & Strategy at Bath University and Canterbury University, NZ, research fellow of the Bristol University Systems Centre. Principal of Systemic Consulting and has experience of implementing risk systems in insurance and civil engineering organisations. Played a leading role in the research & development of STRATrisk.

Roger Allport, civil engineer and transport economist, has spent his career in consultancy (Halcrow) and research (Imperial College London), working in the fields of urban transport policy and major project development in the UK and Asia. Member of the civil engineering and actuarial professions' risk working groups and leads on operational risk.

Alison Brown, Faculty Manager, Engineering Policy and Innovation, Institution of Civil Engineers. Secretary of this Group.

Chris Chapman is Emeritus Professor of Management Science in the School of Management at the University of Southampton. He has designed risk management processes adopted by many organisations world wide. He was the Founding Chair of the Project Risk Management Special Interest Group of the Association for Project Management, and he is a Past President of the Operational Research Society.

Michael Clark, actuary. Michael chairs the Risk Analysis and Management for Projects initiative between the actuarial and civil engineering professions. His work at Shell involves corporate structuring, valuation and risk assessment for new projects; he led the $5.3bn financing of the world's largest oil & gas project on Sakhalin island in Russia about which Project Finance Magazine commented, "the deal deserves to be a case study for the financing of large extractive industries projects. Few others have managed to combine environmental, construction and political risks in such a dramatic fashion".

Roger Dix is an actuary, who now works for Ernst & Young in their Financial Services Risk Management team. Prior to this, he worked for several life insurers and reinsurers, mainly on corporate and risk related work

Jerry Greenhalgh FRICS. Jerry is a member of the ICE/ICES Management Panel, also serving on the RAMP and ERM Working Groups. His career as a senior commercial manager with Costain spanned over 40 years. He now has his own company providing commercial consultancy services to the construction industry.

Clive Hopkins is Head of M&A - London, Treasury and Corporate Finance, Shell international Limited. Clive is an actuary who has worked for Shell for 32 years, initially as Pensions Manager, when he was also Vice Chairman of the NAPF. Clive subsequently took up positions as Head of Investor Relations, and then CFO of Shell UK Downstream, where he was Chairman of Colas Industries. He was Head of Project Finance for five years before taking up his present role. Former Chair of the Joint Working Party on RAMP.

Chris Lewin, actuary. Chris leads the joint risk-management initiative between the actuarial and civil engineering professions. He has spent most of his career in pensions management, notably at British Rail, Guinness and Unilever, and is currently a member of the Investment Committee at The Pensions Trust. Chair of this Group and former Chair of the RAMP working party. Editor of this Guide.

Mike Nichols, Chairman & CE of Nichols Group, Chairman of Association for Project Management, Board Member of Major Projects Association, and Member of Standards Policy & Strategy Committee of BSI. Specialist in project, programme and portfolio management. Played leading role in development of RAMP and STRATrisk.

Professor Tony Ridley, civil engineeer, a Past President of ICE and former HoD at Imperial College London, was a co-founder of the civil engineering/actuarial risk management initiative. He has held Chairman/Board/CEO positions with transport organisations in Newcastle, Hong Kong and London, and has been a Board member of the MPA and Chairman of the APM.

Mark Symons, Barrister-at-Law, is Practice Manager, Enterprise Risk Management, The Actuarial Profession, charged with helping to gain recognition for actuaries as leading professionals in the field of ERM. Previously, Mark was in representational work with trade associations and industry bodies including the CBI.

Gordon Wood, actuary. Ernst & Young.