# GOVERNANCE AND RISK MANAGEMENT IN UNITED KINGDOM INSURANCE COMPANIES

S. P. Deighton, R. C. Dix, J. R. Graham and J. M. E. Skinner

[Presented to the Institute of Actuaries, 23 March 2009]


## ABSTRACT

For some while there has been a growing awareness from both internal and external stakeholders that the governance and risk management in United Kingdom (U.K.) insurance companies needed to be enhanced. The proposed European Union Solvency II Directive makes this very explicit and the current economic turmoil has put a much stronger emphasis on the whole process: it is being seen as the right thing to do, rather than simply a regulatory requirement. In this paper, we set out the background to and recent history of governance for U.K. insurance companies, and consider how enterprise risk management can bring together the various control frameworks needed to support that governance. Whilst no two companies are the same, and hence the solutions to these issues will vary, there are several common themes linked to successful implementation. Similarly, various barriers to success are identified, together with solutions to resolve them.



## KEYWORDS

Corporate Governance; Risk Management; Enterprise Risk Management (ERM); Solvency II; Turnbull; Combined Code; Chief Risk Officer; Internal Controls; Listing Rules; Sarbanes-Oxley; Financial Reporting Council (FRC); Rating Agencies; Internal Audit; Strategy



## CONTACT ADDRESS

S. P. Deighton, M.A. F.I.A., Just Retirement Ltd, Vale House, Roebuck Close, Bancroft Road, Reigate, Surrey RH2 7RU U.K., Tel: +44(0)1737 233380;
E-mail: shayne.deighton@justretirement.com


## 1. Introduction

1.1 This paper, while touching on some of the benefits of enterprise risk management (ERM), (see Appendix A for a brief discussion), is not intended to make the business case for it. Rather it starts from the assumption that it is seen as desirable, then considers how it fits within the wider control environment of a company. It is clear that scope exists for confusion about governance, financial controls, compliance, risk management, internal

controls etc. How do they relate to each other and who is responsible? This paper aims to give that background.

1.2 In particular it concentrates on placing risk management in the wider context of corporate governance and internal control frameworks, with which many actuaries will not have had cause to come into contact. It is not a technical paper on risk management, nor does it contain original research on technical subjects. However, its key theme is that technical skills are a necessary but not sufficient pre-requisite for actuaries to make a major contribution to risk management in financial institutions.

1.3 Section 2 gives a brief high level overview of various aspects of control and governance.

1.4 Section 3 provides a summary of the background and detail of the U.K. corporate governance framework.

1.5 Section 4 sets out details of the current regulatory control regime for U.K. insurance companies, and its expected future form, Solvency II.

1.6 Section 5 describes the governance framework required to assist management in identifying, measuring and managing risks.

1.7 Section 6 then describes various aspects of implementation of ERM, with a particular focus on key enablers for success.

1.8 Section 7 gives details of some known barriers to successful implementation, and how they can be mitigated.

1.9 This paper has been written under the auspices of the Enterprise Risk Management Practice Executive Committee (ERM PEC).

## 2. Governance, Control and Risk Management — A Brief Overview

### 2.1 *The Nature of Corporate Governance*

2.1.1 The limited liability concept and the complex structure of the capital markets which have grown up around it ranks as one of mankind's greatest inventions. It allows us to undertake manufacturing, research and development on a scale which would be simply inconceivable for individuals or even groups of people acting alone. It underpinned the industrial revolution and has been just as important in the evolution to the technology and service-based markets of today. However, the very paraphernalia of the capital markets, from vast electronic exchanges at one end of the spectrum to the ability of individuals to make small investments in Individual Savings Accounts (ISAs) at the other, conspire to make it surprisingly easy to forget what is actually going on; one group of people is handing its money to another group of people to do business with, whatever that may be. This is done in the hope of receiving a good return for so doing: the counter side being that (hopefully) it is understood that any business venture carries some risk. The group may not get as good a return as it had hoped. In some circumstances it may even lose all of its investment.

2.1.2 However, whilst acknowledging the vagaries of business, what these people would *not* expect is that the people to whom they entrust their money will use it without due care and attention. They expect the business to be conducted broadly in line with whatever representations were made to them, and do not expect their money to be used in other irresponsible or speculative ways. They expect the managers to exercise an appropriate degree of skill, expertise and care. They expect to be kept informed of what is going on, and to get regular indications of the return being achieved.

2.1.3 In short, investors need a system of 'corporate governance'. This was defined simply in the Cadbury Report (1992: S 2.5) as: "the system by which businesses are directed and controlled", although there is no single agreed working definition. The system of governance can either be enforced by legislation or by self-regulation, or (as in the U.K.) by a combination of both.

## 2.2 *Financial Controls*

Perhaps not surprisingly given what was said above, one of the areas of corporate operations which has been subject to much scrutiny from the earliest days has been the treatment of the money handed over. What has happened to the cash: where is it held; what has it been spent on; what profit has been made; when can we expect to see some of it returned? A company without the basic disciplines to answer these questions would not be trusted. Companies have, therefore, developed financial control frameworks to ensure they can track the cashflow and the profits properly, and can make reliable reports of progress to shareholders (provision of reliable accounts is one of the primary legal duties of a company's directors). The auditing profession and audit standards have developed in parallel to provide external assurance on these financial controls.

## 2.3 *IT Controls*

These days most of the financial records 'live' inside computer systems. In fact, many of the company's processes depend heavily on information technology — manufacturing plant is often computer controlled; and financial services are dependent on sophisticated contract administration and dealing systems. A malfunction, error or complete outage of such systems can have severe impacts on a company's finances and reputation. So, again, it is not surprising that a whole range of controls have grown up around information technology (IT) and, indeed, a separate language has developed (see for example Control Objectives for Information and related Technology ('COBIT') published by the IT Governance Institute).

## 2.4 *Compliance*

2.4.1 Insurance companies are subject to a much higher level of scrutiny

than ordinary trading companies because customers pay their premiums before the final product or service is delivered to them, and this money needs to be protected. Typically, they are subject to an additional body of law, and are monitored by government or by independent regulators. For multinationals there may be many regulators involved. This is explored in more detail in Section 4. Regulation may be of three types:

(a) prudential (i.e. solvency);
(b) conduct of business; and
(c) product.

There may also be trade bodies with their own particular requirements.

2.4.2 The penalties for failing to meet these regulatory requirements can be severe, so most U.K. companies have created "compliance" departments specifically to police them.

2.4.3 In many companies compliance would also be deemed to cover other types of regulation, for example Health and Safety. It may also cover fraud and financial crime, although some companies have a separate dedicated team for this.

### 2.5 *Business Protection*

There are two aspects to this, which some companies treat as separate issues. The first is protection of the company's assets, which would include people and intellectual property as well as physical assets. The second is business continuity, in other words enabling the business to continue to function after a major incident, whether that be a result of nature, supply failure or terrorism. Both of these are often seen as very closely linked with IT controls, but it would be wrong to think that IT can cover all the issues. It is not the intent to go into these in detail in this paper, rather to note that these can also be thought of as part of the wider internal control framework.

### 2.6 *Internal Controls and Risk Management*

2.6.1 Companies of all types take a number of inputs or resources (capital, people, fixed assets, brand, intellectual capital) and use them to achieve certain outputs or objectives, (e.g. dividends, debt repayment, growth). In order to achieve the objectives the company must expose the resources to certain risks. Alternatively the objectives can be seen as the reward for taking those risks. The company must make critical decisions on:

(a) the level of risk to which it is prepared to expose its resources in order to achieve its objectives;
(b) the level of risk which it is prepared to accept of *not* achieving its objectives; and
(c) whether the level of potential reward is consistent with the risks.

2.6.2 In current jargon, this would be referred to as the company's *risk appetite*. Unfortunately it is often the case that in order to achieve the objectives the company might undertake activities which expose the resources to risks which are beyond its risk appetite. The company then has three options:

(a) find an alternative approach to achieving the objectives that allows it to avoid those activities and hence the risks;
(b) put in place some sort of mitigating process which reduces the impact of the risk if and when it crystallises; or
(c) put in place some sort of mitigating processes which are designed to reduce the likelihood of the risk crystallising.

2.6.3 Option (c) would be what many would recognise as *internal controls*, but in reality they are the combination of all three. It should be clear that the financial and IT controls referred to above are no more than specific examples of internal controls. Some companies also explicitly recognise certain other activities, such as security, business protection, business continuity, fraud and money laundering, all of which are just further examples of internal controls.

2.6.4 It is important to note that an internal control cannot remove a risk altogether (even Option (a)) and therefore ensure that a company achieves its objectives with no unintended destruction of resources. It only provides a certain level of assurance, and there is a clear trade-off between the cost of the control process chosen and the level of assurance achieved.

2.6.5 A simple definition of risk management is as a process which pulls together the steps outlined above with the aim of giving a company a chance of achieving its objectives with a chosen level of confidence, for example:

(a) identify resources and objectives, create a strategy to achieve the objectives and plan in detail to implement it;
(b) set a risk appetite;
(c) identify all possible risks to the resources and the objectives ("inherent risk");
(d) implement internal controls to address the risks deemed outside appetite;
(e) assess the nature of the risks given the controls, including allowing for the possibility that the controls fail ("residual risk");
(f) assess the effectiveness of the internal control framework in action; and
(g) provide regular reporting on the risks and the effectiveness of the framework.

This is of course an iterative set of processes.

2.6.6 The link between strategy and risk cannot be over-emphasised. Risk and reward go together; this is true for any company, but nowhere is it

more explicit than in an insurance company. In creating its strategy, a company must be very clear on the rewards it believes are available — the greater the potential reward, the greater the level of risk appetite that might be justified, and vice versa.

2.7 *Enterprise Risk Management*

2.7.1 There is no doubt that one of the biggest changes in the corporate world in the last ten to15 years has been the emergence of risk management as a separately recognisable function. This has been particularly true in the financial services sector but other industries have also contributed much to its development (for example energy, pharmaceuticals, civil engineering). More recently we have seen the development of the concept of enterprise risk management.

2.7.2 This is not to suggest that companies were previously not practising risk management, just that it was undertaken intrinsically as part of a line manager's role, often in a 'seat of the pants' way and unconnected to the risk-related activities of other managers. Also, there would have been little formal record of how risk was being handled, and probably no centralised reporting of the risks being run. It is also true to say that, although the financial sector has been clearly leading, much of the development in that sector has focused not on the day-to-day definition of risk (i.e. the chance of things happening that hurt us) but on the more esoteric financial economics meaning of (statistically measurable) volatility.

2.7.3 A key differentiator of enterprise risk management is looking at risks of all types in a holistic way; in other words, looking at risk from the perspective of the whole company (but not necessarily in just a top-down way), and looking at how risks of various types (and across various geographies) interrelate with each other. This leads, naturally, to the concept of diversification benefits: the extent to which the capital required to support a company's risks' viewed in aggregate, may be less than the sum of the capital amounts required to support the risks viewed individually.

2.7.4 Another is to look at positive as well at as negative risk, and to ensuring that risk management is an intrinsic part of the strategic management of the company (in other words, stressing step (a) above).

2.8 *Management versus Oversight*

Section 5 describes in detail the difference between risk management and risk oversight. In reality, the distinction between these two activities is not always clear cut. One source of confusion is that those within a company charged with risk oversight are often referred to as the risk management department, whereas this paper argues that responsibility for risk management lies primarily with line management. Throughout this paper we

have used the common terminology and have tried to make the context clear as to whether we mean management or oversight.

## 3. The U.K. Corporate Governance Framework

### 3.1 *Limited Liability and the Need for Corporate Governance*

3.1.1 Anyone coming to the subject of corporate governance for the first time is faced with a bewildering array of names and acronyms: Companies Acts, Turnbull, FRC, FSA, Combined Code, UKLA, Sarbanes-Oxley, Higgs, Cadbury etc. The aim of this section is to place these into context by looking at the way in which corporate governance has developed in the U.K., with some reference to developments in the United States of America (U.S.).

3.1.2 The concept of limited liability was mentioned in the introduction and forms the basis for the vast majority of (but not all) corporate bodies in the U.K. Under such a corporate structure there is an inherent tension between shareholders and management which is often referred to as the 'agency problem'. Essentially the problem is that the interests of shareholders and management may not be properly aligned, leading to sub-optimal decision making and the destruction of value. This will be familiar to actuaries from the development of market consistent embedded value techniques, where it may be suggested that a deduction from value should be made to allow for its impact.

3.1.3 In reality, the problem is more complex; there are three 'players' in the game. The directors of a company are, as a group, responsible to the shareholders for managing their company. However, they themselves delegate the day-to-day running to another group, the executive management, which may imply some overlap since some directors are themselves executives. So, there are two levels at which agency issues *can* arise. However the common view is probably that the directors are charged with exercising governance over the management on behalf of the shareholders.

3.1.4 The agency issue also arises in other types of company. Most familiar in the U.K. would be the mutual, where policyholders have an analogous role to shareholders, and similarly have no liability beyond what they have invested with the company. It is also relevant for companies which have no external shareholders, but which are wholly owned within a group structure, particularly when such a company is a regulated entity.

3.1.5 Despite the evident success of the limited liability system, by its very nature it encourages risk-taking and there have been many corporate failures around the world. Some of these have been large enough, and involved issues serious enough, to shake confidence in the system, and, consequently require action. In the 1980s and early 1990s in the U.K., there were a number of corporate collapses and scandals:

| | | |
|---|---|---|
| (a) | 1987 Guinness | (false accounting; theft) |
| (b) | 1988 Barlow Clowes | (fraud) |
| (c) | 1990 Coloroll | (over-expansion; over-leverage; accounting irregularities) |
| (d) | 1990 Polly Peck | (over-leverage; no internal controls; false accounting) |
| (e) | 1991 Maxwell | (over-leverage; share price manipulation; abuse of pension scheme funds) |
| (f) | 1991 BCCI | (a wide range of illegal activities, false accounting and control breakdowns). |

3.1.6 During the 1990s, attention was focused on a number of derivative-related controls breakdowns, the most spectacular being the demise of Barings Bank in 1995

3.1.7 Just after the turn of the millennium there was a further wave of corporate scandals which were worldwide news (Enron, WorldCom, Parmalat). These prompted immediate and significant response, in the U.S. in particular. Closer to home we had Independent Insurance and Equitable Life.

3.1.8 As we began to write this paper in the Autumn of 2008, the global financial system was clearly in turmoil as a result of issues arising from the so-called 'credit crunch'. However, even at that stage few could have imagined the events which would unfold over the three months or so it took to complete. We had seen the bankruptcy of one major bank, but have now seen bailouts of both the world's largest bank and largest insurer, the U.K.'s biggest mortgage lender being taken over, and government intervention to shore up the banking system in nearly every major economy in the world. Whilst there is, as yet, no implication of actual wrongdoing at any of these institutions, it is clear, with hindsight, that they were being run with a much higher exposure to risk than their owners, and, perhaps, also their management, realised. For some this was through lending to overstretched private mortgagees or property developers, for others through buying asset-backed securities many times removed from the underlying risk, and for others from exposure to credit default swaps. With many accounting and regulatory systems now operating on a mark-to-market (or model) basis, the dramatic widening of credit spreads has damaged the capital bases of other institutions, even if they did not indulge in these practices.

3.1.9 As a result, it is quite probable that we will see another round of developments on the regulatory and corporate governance front in the near future. Lord Turner, Chairman of the FSA, indicated in a recent speech (2009), that this is not a probability, but a certainty, the only question being what form this will take.

### 3.2 *Brief History of Corporate Governance Development in the U.K.*

3.2.1 It is perhaps, surprising to find, given the importance of corporate

governance, that it is not driven directly by legislation in the U.K. Whilst the Companies Acts set out the basic framework and rules for the creation and operation of limited liability companies, they do not deal directly with all the issues arising from the agency problem. In fact, prior to 1992 there was nothing explicitly giving guidance on this.

3.2.2 This is not to say that companies did not practice 'corporate governance' up to that point. Rather, companies adopted practices which were deemed 'right' for them, proportionate to their size and complexity. Via the influence of joint directors, auditors, etc., the best of these practices would have spread from company to company. However, typically, companies would not have communicated much in public on their corporate governance practices.

3.2.3 Following the scandals involving Maxwell and BCCI in 1991, there was clearly a need for a more explicit approach to corporate governance, in order to restore confidence. A committee was formed under the chair of Sir Adrian Cadbury, sponsored by the Stock Exchange and the accountancy profession, which reported in 1992. The report included a proposed Code of Conduct.

3.2.4 The Stock Exchange added a requirement to its Listing Rules that companies should state whether they had complied with the Cadbury Code of Conduct (1992) or, if not, explain why not. This was the start of the U.K.'s 'comply or explain' approach to corporate governance, which is still in place today, and which contrasts in particular, with the direct regulation approach adopted by the U.S.A.

3.2.5 The Cadbury Report (1992) looked at a number of key issues:

(a) relationship between chairman and chief executive;
(b) role of non-executive directors;
(c) reporting on internal controls; and
(d) financial reporting.

3.2.6 In 1995, a follow-on committee (Greenbury) looked in detail at the issue of directors' remuneration.

3.2.7 The Cadbury and Greenbury recommendations were brought together in 1998, via the work of the Hampel Committee, in the first Combined Code (1998). The Code has remained the overarching document ever since and the precedent had been set for specialist committees reporting on areas of detail, followed, at some point, by a Code update — hence the proliferation of names in the corporate governance arena.

3.2.8 A particularly important example at this time was the creation of the Turnbull committee. This was created because the Code (1998) required directors to conduct a review of the effectiveness of the company's systems of internal control, but there was no available explicit framework for so doing. The report "(*Internal Control: Guidance for Directors on the Combined Code*") was issued in 1995 and provided such a framework. It was revised in 2005.

3.2.9 Following the demise of Enron and Worldcom, 2003 was another busy year. Three specialist committees reported: Higgs on the role of non-executive directors, Smith on the role of the audit committee and Tyson on the recruitment and development of non-executive directors. These were incorporated in another Combined Code update (2003). By this time, responsibility for publishing and maintaining the Code had been passed formally to the Financial Reporting Council.

3.2.10 The Combined Code was revised again in June 2006 and the latest version was released as recently as June 2008, applying to accounting periods starting after 29 June /2008.

3.2.11 Having moved quickly through the history, the next section looks in some detail at the current environment.

### 3.3 *The Current Environment for U.K. Listed Companies*

The legal and governance environment for a U.K. listed company consists of the Companies Acts, the Listing Rules, the Combined Code (June 2008) and the Turnbull Guidance (October 2005). If the company has a U.S. listing, it will also be subject to the Sarbanes-Oxley Act of 2002 ('Sarbox'). In the rest of this section we look at these requirements in more detail, and also examine the role of the various parties involved in corporate governance.

### 3.4 *Companies Acts*

3.4.1 The Companies Acts have existed in the U.K. in some form since the middle of the nineteenth century. They set out the framework in which limited liability companies of all forms must operate. In recent years, the Government has undertaken a complete bottom-up review of the legislation, culminating in the Companies Act 2006. This replaces the 1985 Companies Act, although the level of change is such that implementation has been spread over the period to October 2009, to give companies time to prepare. The Companies Act (2006) covers type of company, formation and naming, rights of members, directors' duties, accounts and audit, capital and distributions, takeovers and mergers, and offences.

3.4.2 The key change from a governance viewpoint is that it has been made explicit that directors should no longer think only about the interests of the company, but must also consider the wider impact of their decisions, for example on employees or the environment.

### 3.5 *The Listing Rules (LR)*

3.5.1 These are now maintained and enforced by the FSA, which for this purpose may sometimes refer to itself as the U.K. Listing Authority. They should be taken together with the Prospectus Rules and the Disclosure and Transparency Rules (DTR), all of which form part of the FSA Handbook.

3.5.2 Most relevant, from a corporate governance viewpoint, are require-

ments to treat all shareholders equally and the rules on the use and the abuse of insider information.

3.5.3 The requirement to 'comply or explain' with the Combined Code (2008) is set out in LR 9.8.6R(6). The requirement to have an audit committee is now set out explicitly in Disclosure Transparency Rule (DTR) 7.1 (i.e. it does not rely on compliance with the Code), in order to meet requirements of the European Company Law Directives.

3.6 *Combined Code*

3.6.1 The four key areas of the code are:

(a) directors;
(b) remuneration;
(c) accountability and audit; and
(d) relations with shareholders.

3.6.2 There is also a separate section aimed at institutional shareholders, recognising the important role which they have to play in monitoring and in influencing companies' behaviour.

3.6.3 The Code requires that companies should be headed by an effective board, which is collectively responsible for the success of the company. The roles of the chairman and CEO should be split, so that "no one individual should have unfettered powers of decision", and similarly there should be a balance of executive and non-executive directors. There should be a rigorous and transparent procedure for appointing directors, who should receive a proper induction and regular skill/knowledge refreshment. The board should evaluate its own performance annually, both collectively and individually, and maintain a plan for its 'progressive refreshing'.

3.6.4 Remuneration should be sufficient to attract and to retain the right quality of directors, but it should not be excessive. A significant proportion should be linked to corporate and individual performance. There must be a policy for remuneration, and no directors should be involved in deciding their own pay.

3.6.5 The board should present the shareholders with 'a balanced and understandable assessment of the company's position and prospects'. It must maintain a sound system of internal control, and review it at least annually. An audit committee should be established, consisting entirely of independent non-executive directors.

3.6.6 The board, as a whole has a responsibility for ensuring that a satisfactory dialogue takes place with shareholders, with a constructive use of the AGM. A senior independent director must be appointed and be available to shareholders.

3.6.7 Section 2 of the Code on Institutional Shareholders (2008: 21) requires them in turn to maintain a dialogue with the company based on "the mutual understanding of objectives". They are reminded of their

responsibility to make considered use of their votes. (Note: companies are only required to state compliance with Section 1).

3.7 *The Turnbull Guidance*

3.7.1 Turnbull (1999) is a principles-based document, aimed at describing a framework, rather than a set of precise guidelines, on how to set up internal controls. It is intended to address Principles C.2 of the Code on Institutional Shareholders:

> "The Board should maintain a sound system of internal control to safeguard the shareholders' investment and the company's assets'') and C.2.1 ("The directors should, at least annually, conduct a review of the effectiveness of the group's system of internal control and should report to shareholders that they have done so. ...''

of the Combined Code (2008) and the reporting requirements of paragraph 9.8.6 of the Listing Rules.

3.7.2 It is not appropriate to go through the guidance in detail here; it is not a long read and we would recommend interested readers to look at the original. The following observations are worth noting:

(a) it recognises compliance, financial controls and operational effectiveness as just elements of an overall internal control framework;
(b) it stresses that internal controls can only manage or control risks, not eliminate them;
(c) internal controls should be 'embedded in the business';
(d) all employees have some responsibility for risk management;
(e) risks change continuously — so must the controls;
(f) control failures must be analysed, acted upon and reported upon(*); and
(g) culture, HR policies and performance rewards must support risk management and internal controls.

3.7.3 Paragraph 36 of the Combined Code (2008) states:

> "... It should also disclose the process it has applied to deal with material internal controls aspects of any significant problems disclosed in the annual report and accounts''. This is potentially somewhat flawed drafting since the decision on what is disclosed in the accounts is driven by a different set of standards, and the result can be that fairly serious control issues are not brought to light because the financial impact of them does not trigger a requirement for disclosure elsewhere in the accounts.''

3.7.4 Complying with the guidance can be problematic in a group environment, particularly where there are companies, such as joint ventures, where the group cannot exercise full control.

3.8 *Sarbanes-Oxley (2002)*

3.8.1 Properly known as the Public Company Accounting Reform and Investor Protection Act, this was passed in 2002 as a direct result of Enron,

with significant impacts on both companies and their auditors, including the creation of the Public Accounting Oversight Board. Its most publicised requirement is that the CEO and the CFO of public companies have to take personal responsibility for the financial statements, and to certify that they do not contain any untrue statement of a material fact. They are also responsible for establishing and maintaining an effective system of internal controls (note that in Sarbox this means just financial controls).

3.8.2 The biggest workload in complying with Sarbanes-Oxley (2002), which has affected many U.K. companies with U.S. parents or secondary U.S. listings, comes from Section 404. This requires a statement in the annual report that management is responsible for the internal control framework and processes for financial reporting, and for an assessment at the year end of their effectiveness. This assessment must be accompanied by an attestation from the company's auditors.

3.8.3 The U.S. approach can be seen as rules based with enforced compliance, a complete contrast to the U.K.'s principles-based 'comply or explain' regime.

### 3.9 *The Role of the Financial Reporting Council*

3.9.1 The Financial Reporting Council ('FRC'), formed in 1990, is: "the U.K.'s independent regulator responsible for promoting confidence in corporate reporting and governance''. It has, of course, become significantly more familiar to the majority of actuaries recently as the top level organisation for setting actuarial standards and for the professional oversight and discipline of actuaries. It is not a government organisation, although the Chairman of the FRC Board is appointed by the Secretary of State for Business, Enterprise and Regulatory Reform. It is funded by levies on all listed companies (including AIM and PLUS), and now also on insurance companies and pension schemes (in relation to oversight and standard setting for actuaries).

3.9.2 The FRC operates primarily through its five operating bodies (Accounting Standards Board, Auditing Practices Board, Board for Actuarial Standards, Professional Oversight Board, Financial Reporting Review Panel, Accountancy and Actuarial Discipline Board), and, in addition, there is a Committee for Corporate Governance (actually a sub-committee of the FRC Board) supported by a separate Corporate Governance Unit.

3.9.3 The Committee monitors the operation of the Combined Code (2008) and its implementation by listed companies, and reviews developments in corporate governance generally. It has held this responsibility since 2003. It may from time to time instigate reviews of specific aspects of corporate governance as a result of this. Any resulting recommendations for changes to the Combined Code (2008) are then approved by the main FRC Board. The Committee also produces guidance on the application of the Code (for example Turnbull).

3.10 *The Role of the Board, its Members and Committees*

3.10.1 U.K. companies operate under a 'unitary' board framework, in contrast to the model in certain European countries of separate management and supervisory boards. It is important to distinguish between the responsibilities of the board as a whole and those of the directors as individuals. The board is responsible in law for the successful stewardship of the company, and has a fiduciary responsibility to its shareholders, and only to its shareholders. It is also absolutely clear that the board has primary responsibility for the control of the company, encompassing all the areas discussed in this paper (internal & financial controls, risk management, compliance). Whilst day-to-day activity in these areas can be delegated to management, responsibility remains with the board.

3.10.2 There is a conflict between these two goals of the board, which contributes to the agency issue identified in the Introduction. This is one of the reasons why it is important that there is a good balance on the board between executive directors (likely to be remunerated for driving the company forward and profits) and non-executive directors (who are typically fee based). It should be noted that there is a further distinction between non-executive directors who are deemed 'independent' and those who are not. Independent directors are defined in Cadbury (1992: S4.12) as those who "*... apart from directors' fees and shareholdings [are] independent of the management and free from any business or other relationships which could materially interfere with the exercise of the independent judgement.*" Legally, there is no distinction between the three types of director.

3.10.3 Following the recommendations of the Smith Report, all listed companies must now have an audit committee. This is a sub-committee of the board comprising only non-executive directors. Executive directors and other senior management can, and usually do, attend meetings, but only at the invitation of the committee (an exception to this may be the head of internal audit, and increasingly, the chief risk officer, who may be granted the explicit right to attend and to be heard).

3.10.4 The demands on Audit Committees have become increasingly onerous and many found it was difficult for them to complete their business in the scheduled meetings. Many companies have therefore formed separate Risk Committees, either as a sub-committee of the Audit Committee or as a separate sub-committee of the Board. In either case it would usually have formal delegated authorities and responsibilities from the Audit Committee. The Risk Committee would normally be responsible for the internal control system and reviewing its effectiveness, including risk management and compliance, and would review regular risk reporting from management. The responsibility might extend to financial controls, or these might be left with the Audit Committee.

3.10.5 The duties and responsibilities of individual directors arise from the Companies Acts. The Company Directors' Disqualification Act 1986 is

also relevant. Directors may be subject to both civil and criminal prosecution. Individually, directors do not have the authority to commit the company, unless such authority has been formally delegated to them by the board.

3.11 *The Role of Senior Management*

3.11.1 It is clearly not practical for the board, which includes non-executive members, to actually perform the day-to-day management of the company, to develop and to maintain the system of internal control or to undertake risk management. This is, therefore, delegated to the executive directors and the other senior management. Typically, this is channelled via a formal letter of *delegated authority* to the CEO, who would then issue similar letters to other executives, cascading down from there. As an aside, this existing practice has been formalised in the FSA's Approved Persons regime.

3.11.2 Individuals at all levels in an organisation should have a role profile, which sets out the general nature of their job, its key parameters and what is expected of them. This is not quite the same as a delegated authority, which is a more definitive list of what an individual must and must not do, and would set out, for example, monetary limits on decisions and committing the company, although, in some organisations, they might be combined. Only more senior individuals would usually have a delegated authority letter.

3.11.3 Senior managers are usually, and quite rightly, remunerated on results. For executive directors, it is actually a requirement of the Combined Code (2008). This can cause direct conflicts with their responsibilities from a governance/risk management viewpoint. This is explored more in Section 6 below.

3.12 *ERM as a Consolidating Framework*

3.12.1 The annual requirement under Turnbull (1999) for the directors to conduct a review of the effectiveness of the company's internal control systems, and to report thereon to shareholders can be a fraught process for a company which still approaches risk and control in a silo-based way. Similarly changes to U.K. and international accounting standards in recent years have greatly increased the amount of disclosure required in the report & accounts in relation to risk and control, and, in many cases, the process for producing these disclosures has not been developed. Typically, there will not be any single person or team with an overall view of the governance and the control systems of the many types which we have discussed. The review and the production of the disclosures, therefore, becomes a very disjointed process.

3.12.2 We have described ERM as a process that considers risks and controls of all types in a holistic way, looking at risk from the perspective of

the whole company, and looking at how risks of various types interrelate with each other. Also, ERM looks, not just at the risks themselves, but at the management actions and reporting associated with them as well. ERM is, therefore, a readymade consolidating framework for the collation of the review and reporting, such as that required by Turnbull (1999). Equally, the CRO would be the natural candidate, maybe alongside the CFO, to present that review to the board for sign-off.

3.13 *Rating Agencies*

3.13.1 The rating agencies have always, almost by definition, taken an interest in risk management within the companies which they rate, but this tended to be implicit in their overall approach. In recent years, their focus on this has become more explicit, and, to some extent, this has paralleled the wider emergence of ERM.

3.13.2 In 2005, Standard and Poor's included a formal evaluation of ERM as the eighth pillar of its rating process, and since then has published various articles detailing how it approaches this assessment (its 2006 paper "Insurance Criteria: Refining the Focus of Insurer Enterprise Risk Management Criteria'' being the main one). Its approach focuses on five key areas of the ERM framework: risk management culture, risk controls, emerging risk management, risk and capital models, and strategic risk management. It carries out senior level interviews, review relevant documents and reports, and also conducts site visits in the business to observe risk management in action and to assess the quality of the risk teams. Based on this it arrives at an ERM classification:

(a) weak (ERM program cannot consistently control all of an insurer's major risks) — 4% of worldwide insurers in 2007;
(b) adequate (ERM programs have fully functioning risk control systems in place for all major risks) — 83% of insurers;
(c) strong (ERM program exceeds the adequate criteria for risk control, and the company has a vision of its overall risk profile, an overall risk tolerance, a process for developing the risk limits from the overall risk tolerance which is tied to the risk-adjusted returns for the various alternatives, and a goal of optimising risk-adjusted returns) — 10% of insurers; and
(d) excellent (ERM programs share all the criteria for programs considered strong, but are more advanced in their development, implementation, and execution effectiveness) — 3% of insurers.

Overall, U.S. insurers scored better than their U.K. and European counterparts.

3.13.3 A.M. Best takes a slightly different approach to ERM. Its 2007 paper "Risk Management and The Rating Process for Insurance Companies'' notes that "*A.M. Best will consider allowing companies to maintain BCAR*

*(i.e. capital) levels below the guideline for their ratings based on a case-by-case evaluation of an insurer's overall risk-management capabilities — relative to its risk profile.*" So, rather than having ERM as an explicit part of its analysis, A. M. Best considers it as being implicit in all areas of the review process.

3.13.4 For the major listed insurers in the U.K. and on the Continent, maintenance of the current rating would be viewed as extremely important and may appear explicitly as part of the overall group risk appetite statement.

## 4. U.K. Insurance Environment

### 4.1 *The Need for Additional Regulation*

4.1.1 While all companies are exposed to risks of one type or another, insurance companies are one of the few businesses which actively seek to increase their risk exposure. Indeed, their *raison d'etre* is to allow their customers to transfer their own risks to the company. As a result, the insurance industry has been analysing and assessing certain types of risks for centuries.

4.1.2 The last decade or so has seen an emerging emphasis on corporate governance and risk management across all industries. One might expect the insurance industry, and the actuarial profession, to be in their element. However, while the insurance companies are experts in managing transferred risk, many have been relatively slow to embrace broader, holistic risk management, affecting their entire businesses.

4.1.3 Regulators have played a key role in focussing the attention of the financial services industry on risk management. For insurers we now have the Individual Capital Adequacy Standard (ICAS), with Solvency II rapidly approaching: the emphasis being on a holistic risk management process which is embedded in the day-to-day operations of the business, in other words ERM.

4.1.4 Not only has this brought a greater formality to risks which were previously managed in a relatively *ad hoc* manner, but also a greater understanding of risks which were previously thought to be well understood. In addition to looking to measure, manage and place a value on risks of an operational nature we have seen material improvements in the understanding of market risk and longevity risks. This has been aided and abetted by increasing processing power and more sophisticated software.

4.1.5 More sophisticated financial models can develop our understanding of the underlying business risks, but can also introduce their own risks. Models can be wrong, and the more complex the model, the harder it can become to identify situations where this is the case. Moreover, complex models can require many assumptions, implicit and explicit, which create

further degrees of freedom for the user, and heavy reliance on a few key individuals. Blind adherence to a model may be worse than no model at all.

4.1.6 With any model, it is essential that it is tested against the ongoing experience of the business it aspires to model, i.e. an effective control cycle. Moreover, management must be able to rationalise the output of the model, and ensure that it is subjected to proper validation and sense checks. While models may be very sophisticated where certain risks are concerned and based on large amounts of data, (e.g. mortality, market risk) other risks may be modelled in a more approximate way and based on sparse data (e.g. operational risk, correlation between risks). Management must be conscious of the key risks to the business and the robustness of the models in this area.

4.1.7 Despite the increased attention to risk management, there have still been a number of high profile breakdowns within the insurance industry, such as pension mis-selling, endowment mis-selling, payment protection insurance (PPI) mis-selling, lost data and security breaches. Not only do these events attract the attention of people within the industry, they also place it under greater external scrutiny. For an industry which effectively sells a long-term promise to its customers, brand damage can be critical. Moreover, existing and potential shareholders will react negatively to such events, making capital more difficult to source and/or more expensive to reward, and the insurance industry needs capital more than most.

4.1.8 Another unique challenge facing much of the financial services industry is the risk associated with customer decision making, particularly for life insurance business. While all industries rely upon their customers, not many are exposed to the risk of customers suddenly withdrawing their funds or surrendering their policies *en masse*.

4.1.9 Perhaps more worrying is the fact that a 'run on the bank' may be brought about by customers acting irrationally, or based on a misinterpretation of facts, or even based on an unfounded rumour. This reinforces the fact that many of the risks faced by the financial services industry are not well understood externally, or even internally, adding the burden of effective communication of risks and risk management processes to existing challenges. Such information asymmetry may have acted to the benefit of the financial services industry in the past, but can also be to its detriment.

4.1.10 From the customers' viewpoint, the reason they may elect to 'take the money and run', is that they clearly understand the impact which the collapse of an insurer can have on them. This could range from a major reduction in pension provisions, to the inability to meet a claim when it arises. The same applies to other financial services firms, such as banks and investment managers. Shareholders in these types of firm, which operate in a fiduciary capacity in relation to customers' assets, can take advantage of their limited liability, by refusing to put in more capital if the company gets

into trouble, with potentially catastrophic results for those customers. This is sometimes known as the 'shareholder put option'. This option is more valuable if shareholders have access to more information than the customers.

4.1.11 This potential for information asymmetry has heavily influenced the insurance regulatory environment, where much of the emphasis is on requiring insurers to hold sufficient resources to honour obligations to policyholders and the manner in which insurers communicate with their customers. Shareholders will place greater reliance on the requirements of the Companies Act (2006)and the various stock exchanges, on which insurers may be listed.

4.1.12 All industries have a degree of natural conflict between shareholders and customers. In most cases, the customer has a relatively informed choice to make at point of sales, after which the potential for conflict has passed. In the insurance industry, this conflict is ongoing, the most obvious example being the choice between holding higher reserves, (to the benefit of policyholders) or paying a higher dividend (to the benefit of shareholders). Ideally, a company wishes to hold the minimum amount of capital required to meet its risk appetite, and create a win-win situation for shareholders and policyholders alike.

4.1.13 As a result of these influences, many insurance companies have embraced the value adding aspects of risk management. They allow an insurer to avoid or to mitigate certain risks, but also allows the true and complete cost of accepting risk to be included in the prices charged to the consumers. These include risks transferred from the customer to the insurer as part of the contract, and the associated operational risks. The lower the insurer's exposure to operational risks, the lower the charges to the customer, or the greater the profit to the insurer at a given price. Good risk management is emerging as a competitive advantage.

4.1.14 The advantage which the insurance industry and the actuarial profession have is that we have developed the tools to quantify the cost of risk and to charge explicitly for it. We can, therefore, demonstrate the value added by the risk management function.

### 4.2 *FSA Requirements*

4.2.1 Section 3 has described the overall governance framework for U.K. companies in general. This section focuses on the environment in which U.K. insurers operate, and the role played by legislation and the FSA. Financial services companies are governed by the Financial Services and Markets Act 2000 ('FSMA 2000'), with the FSA being responsible for enforcing this act. The FSA has four statutory objectives: market confidence, public awareness, consumer protection and the reduction of financial crime.

4.2.2 The FSA's stated preference for achieving these objectives is '*principles based regulation*' as opposed to pure rules based. The FSA created

and maintains the FSA Handbook which lays down the regulatory requirements for the industries regulated by the FSA. This is an extensive 'living' document aimed at enforcing 11 Principles namely:

Table 1. [FSA Principles for Business]

| | | |
|---|---|---|
| (1) | Integrity: | A firm must conduct its business with integrity. |
| (2) | Skill, care and diligence: | A firm must conduct its business with due skill, care and diligence. |
| (3) | Management and control: | A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. |
| (4) | Financial prudence: | A firm must maintain adequate financial resources. |
| (5) | Market conduct: | A firm must observe proper standards of market conduct. |
| (6) | Customers' interests: | A firm must pay due regard to the interests of its customers and treat them fairly. |
| (7) | Communications with clients: | A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading. |
| (8) | Conflicts of interest: | A firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client. |
| (9) | Customers: relationships of trust: | A firm must take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely upon its judgment. |
| (10) | Clients' assets: | A firm must arrange adequate protection for clients' assets when it is responsible for them. |
| (11) | Relations with regulators: | A firm must deal with its regulators in an open and cooperative way, and must disclose to the FSA appropriately anything relating to the firm of which the FSA would reasonably expect notice. |

4.2.3 '*Principles-based regulation*' involves providing a clear framework and required outcomes, but not necessarily dictating the manner in which the desired outcomes are achieved. The FSA Handbook does, however, incorporate a significant amount of guidance to aid the industry in meeting the principles. The FSA reviews compliance with this framework and acts accordingly where companies fail to comply. It does not look to impinge on the day-to-day running of the company, as may have been common in certain other countries, thereby allowing market forces to drive efficiency and innovation.

4.2.4 This has led to the FSA to being labelled as a 'light touch' regulator, a phrase which is, perhaps, inaccurate and misleading. Anyone who has completed a FSA return, submitted an ICA, or gone through the rigour of an ARROW visit would not consider the FSA touch to be light, nor would the numerous organisations which have been fined or banned from operating.

4.2.5 The preference for principles over rules recognises the fact that organisations are different and have their own idiosyncrasies. Rigid rules will not have the desired effect for many companies, will not create a level playing field, and can allow the exploitation of loop holes. However, while principles allow managements to develop a bespoke approach reflecting the nature of their businesses, it can result in uncertainty as to exactly where the boundaries of complying with any given principle might, or might not, lie.

4.2.6 This is particularly apparent when arriving at the ICA amount. Rules or prescribed scenarios cannot easily capture the specific risks faced by each and every business. However, many insurers continue to battle with the interpretation of the guidance in the Handbook. Moreover, even with principles, a company must create internal rules to produce the required results, more so where practices are to be embedded in the day-to-day management of the business as required by ICAS and Solvency II.

4.2.7 The FSA looks to resolve this by way of ongoing communication. The ICA is submitted to the FSA, who, after review, will either accept the risk-based regulatory capital proposed by the insurer or increase the amount by giving individual capital guidance (ICG): either way, the approved capital number is referred to as the ICG. Where additional capital is required, this has often been down to shortcomings in the operational risk component of the ICA, lack of support for assumptions, or the quality of capital resources. The ICG remains confidential between the company and the FSA to provide a certain amount of leeway for both parties, and will allow the ICA to evolve without undermining market confidence with work in progress driven information. This will not be the case under Solvency II, where regulatory capital add-ons are ultimately expected to be in the public domain.

4.2.8 A company which manages its risk effectively will be rewarded with a lower ICA/ICG, which will allow the company to charge its clients less, or increase return on equity, improving its competitive position (subject to any rating agency capital requirements). This is particularly pertinent for potentially unrewarded risks, such as those of an operational nature.

4.2.9 One very fundamental and fairly prescriptive part of the Handbook is that on "Senior management arrangements, Systems and Controls" (known as SYSC). This could be seen as the FSA emphasising the basic requirements of good corporate governance "*on matters likely to be of interest to the FSA*", and indeed is specifically linked to Principle (iii) above. Firms are required to establish and maintain appropriate systems and controls, and to review them regularly. The first part of SYSC deals in detail with the apportionment of responsibilities to key individuals. The balance deals with the areas or processes where a firm is expected to have adequate controls, or which in themselves act as a form of control, including organisational structure, compliance, employees and remuneration, risk management, MI, internal audit, strategy, business continuity and the keeping of records. The

link with the discussion on governance in Section 3 is clear, and, indeed, SYSC refers to the Combined Code (2008).

4.2.10 Some areas of the FSA Handbook, such as the Conduct of Business Rules, which cover interactions and relationships with customers, do retain a number of more prescriptive rules. These reflect the need to protect the consumer and to recognise the inherent potential conflict of interest between the insurer (and its agents) and its customers.

4.2.11 The FSA has other tools at its disposal to monitor the solvency and the business practices of the financial services industry. Companies are required to submit annual returns; persons holding key roles, such as the actuarial function holder, have to be approved by the FSA, and the FSA visits companies on a regular basis.

4.2.12 One of the tools used by the FSA to assess risk is the advanced risk responsive operating framework (ARROW). This considers both the risks facing specific companies as well as risk themes which may affect a whole industry. The FSA carries out ARROW visits on companies periodically, when they will look to discuss a wide range of risk management issues with key individuals within the businesses. This can include everything from day-to-day risk management processes to solvency calculations. The FSA will take a view as to the degree to which risk and capital management are embedded in the business, the consistency of risk management across the business, the skills of individuals, and the extent to which risk management is being driven from the top (i.e. creating a risk management culture).

4.2.13 The annual returns which insurers currently submit to the FSA include solvency measures based on the existing European Directives, with further requirements for larger with-profits funds. The E.U. driven legislation is referred to as "... *the regulatory balance sheet (or peak I)*" and the additional with-profits legislation referred to as the realistic balance sheet (or peak II). With-profits funds in excess of £500m hold disclosed regulatory capital, which is the higher of the 'twin peaks'. This value is commonly known as the Pillar I capital.

### 4.3 *Solvency II*

4.3.1 For the most part, the approach used to produce the regulatory balance sheet is relatively prescriptive and rules based. The regulatory balance sheet will eventually be replaced by Solvency II. Much of the regulation introduced by the FSA in recent years, such as the realistic balance sheet and ICAS, will play a key role in easing the U.K. insurance industry's transition to Solvency II, whereas many of our European counterparts face a more traumatic journey.

4.3.2 Solvency II is a major piece of European legislation, which is intended to create a revised set of E.U. wide capital requirements, valuation techniques and risk management standards which will replace the current

requirements. In order to negotiate the path to Solvency II successfully, U.K. insurers will need to ensure that their firms live and breathe holistic risk management from chairman to post room.

4.3.3 Solvency II requires insurers to hold sufficient capital such that the probability of insolvency within the next year is no greater than 0.5%, as is the case for ICA. Solvency II is anticipated (at the time of writing) to take effect from October 2012, and is designed to facilitate the development of a single market for insurance services, ensuring a level playing field and a uniform level of consumer protection.

4.3.4 While there are clear similarities between ICAS and Solvency II, many U.K. insurers still have a long way to go to implement Solvency II. The FSA Discussion Paper 08/4: "Insurance Risk Management: The Path to Solvency II", released in September 2008 made this very clear.

4.3.5 While 2012 may seem some way off, Solvency II introduces a range of additional requirements which insurers must implement. The overarching message is that standards will be expected to improve, particularly in terms of embedding the risk management function, and companies' performance in this area will be subject to greater scrutiny, including public disclosures. It will also require changes to the way in which liabilities are valued, including the identification of best estimate reserves and explicit margins, discounting of cashflows for general insurance and a different treatment of options and guarantees from that currently used in most European countries (although not the U.K.).

4.3.6 Many in the industry have expressed a desire that the liability values used for Solvency II be consistent with those required under Phase II of IFRS 4, which is following roughly the same timetable. Life insurers will also be keen to see consistency with the liabilities used in market consistent embedded values (2008), thus reducing the need to calculate, reconcile and explain differing values for what appear to be the same thing. The reality, unfortunately, is that differences seem likely.

4.3.7 The greater disclosure will require firms to publish a solvency and financial condition report (SFC) annually; moreover, any add-ons required by the regulator will also be published. IFRS 4 Phase I (2008) has gone some way to improve the risk related disclosure of insurers; however Solvency II will be more onerous. Under Solvency II there will be no place to hide.

4.3.8 Insurers will be presented with a choice when calculating their solvency capital requirement (SCR), the risk based capital required to reduce the probability of insolvency to 0.5%. They can use a standard model prescribed by the European Commission, they can choose to develop their own internal model or they can use a combination of the two, referred to as a partial model. The Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS) have issued a series of Quantitative Impact Studies (QIS) intended to gather information to allow them to develop a suitable standard model. While completing QIS provides valuable data to

CEIOPS and to the FSA, it also allows insurers to start preparing for Solvency II and to understand how it may affect them.

4.3.9 By June 2009, companies must provide the FSA with their plans to seek approval for their internal models, if they intend to do so. For the larger listed companies one would expect them to develop full internal models. Smaller companies, may be constrained by resource availability and/or the inherent cost of such an undertaking.

4.3.10 It is expected that there will be a financial incentive to use an internal model, in that it will produce a lower SCR than the standard model, and companies may need to weigh up the cost of developing a model against the cost of holding the additional capital. However, the relative costs should not be the only decision driver. Developing a fully embedded capital model which is bespoke to your business is of significant value in its own right.

4.3.11 Anecdotal evidence suggests that the FSA will be a strong advocate of internal models. One can certainly argue that moving from the ICA regime to a standard model under Solvency II would be a retrograde step. Moreover, the standard formula will apply across the E.U. and may not be particularly well suited to U.K. insurers. The FSA will be empowered to insist that an internal model is used where the standard model is not thought to be sufficiently sophisticated to reflect the risks to which the insurer is exposed correctly. One could argue that the standard model producing a lower SCR than an internal model is reason enough to reach the conclusion that the standard model is not fit for purpose.

4.3.12 Each internal model must be approved by the FSA and must run in parallel with the standard model for two years before it can be used alone. A policy must be agreed with the FSA for major changes to the internal model, for which approval is required. Minor changes can be made without approval, the definition of major and minor being agreed with the FSA.

4.3.13 Where companies elect to use a partial internal model, the standard model may be applied to certain business units or to certain risk types. However, the decision must be justifiable from a risk management perspective and not because it produces the most favourable result. In addition, the partial internal model must dovetail with the SCR standard formula.

4.3.14 The E.U. Directive (2008) describes the criteria upon which internal model approval will be based, and while much of this applies to existing ICA models, once again the bar will be raised. These criteria are now discussed briefly.

4.3.15 The *use test* is perhaps the most challenging. Insurers must demonstrate that the internal model is widely used, and plays an important role in their:

(a) system of governance;
(b) risk-management system;

(c) decision making processes; and
(d) economic and solvency capital assessment and allocation processes.

4.3.16 This means that insurers must have in place an effective risk management system, comprising the strategies, processes and reporting procedures necessary to monitor, manage and report, on a continuous basis the risks, on an individual and aggregated level, to which they are, or could be exposed. The risk management system must also consider the risks associated with the internal model itself.

4.3.17 In addition, insurers must demonstrate that the frequency of calculation of the SCR, using the internal model, is consistent with the frequency with which they use their internal model for the other purposes covered above.

4.3.18 As part of its risk management system, every insurer must conduct its own risk and solvency assessment (ORSA). The ORSA must take into account the overall solvency needs: the company's specific risk profile, the approved risk tolerance limits, and business strategy. For example the ORSA might calculate capital requirements on something other than the 99.5th percentile.

4.3.19 The capital requirements laid down by the E.U. Directive (2008) must be met on an ongoing basis, and management must ensure that the internal model remains fit for purpose.

4.3.20 The model must withstand *statistical scrutiny* and the insurer must be in a position to justify the assumptions used by the model.

4.3.21 The internal model must be *calibrated* to calculate the SCR at the 99.5% level as required by the E.U. Directive (2008). If this cannot be demonstrated to the FSA's satisfaction, it can elect to test the model using notional portfolios and externally generated assumptions.

4.3.22 The *profit and losses* experienced by the insurer must be analysed by source to demonstrate how the categorisation of risk chosen in the internal model explains the causes and the sources of profits and losses. The categorisation of risk and the attribution of profits and losses shall reflect the risk profile of the insurer.

4.3.23 The model must be *validated* in terms of how well actual experience relates to the assumptions used, verifying that the model continues to reflect the risk profile of the insurer and is robust to changes in key assumptions, and verifying that the data used are complete and accurate.

4.3.24 Finally, all aspects of the model must be *documented* including:
(a) the design and operational details of the model;
(b) demonstrating compliance with the requirements of the E.U. Directive;
(c) outline of the mathematical and statistical theory and of the empirical basis underlying the model;
(d) the limitations of the model; and
(e) all changes to the model.

4.3.25 Insurers may choose to outsource aspects of the work around the internal model, but this cannot be used as a reason not to adhere to any of the above criteria. Management must take ownership and remain accountable for the model, and ensure that it remains fit for purpose and operates on a continuous basis.

4.3.26 Not only will this be a strain on the resources of the insurance industry, but also on the FSA and other regulators within the E.U. Regulators are required either to approve a model, or to justify their reasons for withholding approval, within six months of the application. Given the volume of potential submissions, this is a Herculean task for the regulators. One of the risks faced by insurers and regulators is that there may not be sufficient skilled resources to go around.

4.3.27 The key messages for U.K. insurers regarding Solvency II are; do not underestimate the work which needs to be done, do not rely upon being able to fall back on the standard model and start work now. Perhaps, more importantly, do not underestimate the value which a fully embedded risk capital model can add to your business.

## 5. Roles and Process in ERM

### 5.1 *Overview*

This section considers the underlying governance required in order to assist management to identify, measure and manage risks. It is written largely from the perspective of a large group, probably with several divisions and many legal entities, but most of the observations also apply to a standalone company. The group board would normally establish a comprehensive framework covering accountability, oversight, mitigation, measurement and the reporting of risk, in order to maintain high standards of risk management throughout the group. This section lays out a selection of roles and responsibilities which could be useful. There is no universal model for this; each group needs to ascertain what works best in its own particular circumstances.

### 5.2 *Roles and Responsibilities*

5.2.1 Risk is not only the responsibility of the risk department. All people employed and engaged by a company must take responsibility for risk if ERM is to be effective. The challenge for any governance system is to ensure that these responsibilities are clear to everyone.

5.2.2 That being said, the starting point for any risk governance must be the board. The board is responsible for setting the overall risk appetite, which should be done in an iterative fashion as part of strategic planning, with the aim of ensuring that the final approved plan is consistent with it. The board will then receive regular information on key performance indicators,

which will indicate, amongst other things, the current level of risk within the organisation and how it compares with the risk appetite.

5.2.3 Whilst risk appetite suggests a maximum capacity for risk, the board should be equally concerned about an under-utilisation of risk, as that would imply the group is not securing the planned reward for taking on that risk. Where credit is being taken for diversification between risks in setting the overall risk appetite, the board should be as concerned about low acceptance of a particular risk as about an excessive acceptance of that risk, because the diversification benefit achieved may be less than that assumed.

5.2.4 The phrase 'risk appetite' is used here to describe:

(a) the level of acceptable risk, given the overall appetite for earnings volatility, available capital, external stakeholder expectations (which could include return on capital), and any other defined objectives, such as paying dividends or particular ratings levels; and
(b) the types of risk which the Group is prepared to accept in line with the control environment and the current market conditions.

5.2.5 Linked strongly to risk appetite is the level of reward able to be received for undertaking each risk. Whilst there might be an appetite for a particular risk, the decision on whether to take on the risk will include an assessment of the expected market reward for that risk. At the strategic level, the Board should make the decision.

5.2.6 Rather than simply having a brief board minute of the decision, it is increasingly common, if not expected and required, for the board to determine and to approve corporate policies on each risk type. These policies will set out very clearly the rationale for the risk decisions made, both in terms of risk which can be accepted, and of any limits upon them. Depending on the overall company structure, the main group policies might need to be replicated at lower divisional levels, with the caveat that the group policies are to be followed at all times. These policies will also include details of who is responsible for setting various aspects of the risk policy, and what governance needs to be followed with what frequency. This should include how any exceptions or carve outs from normal governance will be controlled, and where other third parties may take precedence. This is particularly relevant for a with-profits fund, where the PPFM and with-profits actuary could be examples of this.

5.2.7 Having established the primacy of the Board in the overall risk process, and having approved corporate policies, a methodology is clearly required to embed the process further in the business, and perform the more detailed work. A model which is often used is the 'Three lines of defence' model which is explored in 5.3 below.

5.3 *Three Lines of Defence Model*

5.3.1 This model separates out the tasks of risk management, risk

oversight and risk assurance, calling them respectively the first, second and third lines of defence.

5.3.2 *Risk management* is the primary responsibility of front line managers. They are responsible for identifying and evaluating significant risks to the business, and for designing and operating suitable controls. Internal and external risks are included, although the board's statement of risk appetite is a given in this work. This is the first line of defence.

5.3.3 *Risk oversight* consists of independent oversight of the risks, and the centralised policy management. Centralised policy management can include many items. It can range from the quasi-bureaucratic, such as setting overall policies, standards, and limits, to providing leadership in the development and the implementation of risk management techniques. The overall role can be delivered both in a division, and at a group level. This is the second line of defence.

5.3.4 For the pure oversight part, the key to success is the independence of the people performing the oversight from those whom they are overseeing. For groups who use the three lines of defence model, the greatest differences in approach are often seen in the approach taken to oversight, in particular the balance of oversight between the local division and group. Independent oversight is usually considered to be a two defence, whoever performs that task. (We noted in the introduction the potential for confusion between risk management, the process, and risk management, the department charged with oversight.)

5.3.5 Within a group with several divisions, the centralised policy management sits best within a group function, as that ensures that there is a common methodology for risk management throughout the group. One pitfall to avoid, if this is the case, is that the group performs its policy management in isolation from the rest of the business, without involving the divisions at any time. Given that the ultimate objective is to use common methodologies throughout the group, as part of a wider embedding of ERM, active involvement of all (albeit with the group leading, and having the ultimate controlling vote) is a key factor for success in this field.

5.3.6 *Risk assurance* is the independent assurance from 'neutral' parties that the risk management environment is operating effectively. This is usually provided by the board, and its committees, assisted by the internal audit and the external auditors. This is the third line of defence.

5.3.7 An issue on which companies differ is where the detailed technical quantification of risk sits, and in particular the economic capital modelling. In theory it should sit with the first line, as they are charged with "evaluating" risk. The second line would then review this work, and also provide general guidance on approaches and assumptions.

5.3.8 In practice in insurance companies, partly for reasons of imposing consistency and partly due to the shortage and cost of skilled modellers, this

work is usually undertaken by a combination of the local and the group risk teams, generally comprising actuaries on the life assurance side.

5.4 *Committees*

5.4.1 It is very common that much of the risk agenda is discussed and agreed at a variety of risk committees. This is both good and bad; good, in that there is a clearly targeted and focused agenda to deal with risk issues, but bad, in that risk is perceived to be 'covered' by this committee, and hence no-one else need concern themselves about it. This latter attitude needs to be addressed if ERM is to be successful. Many other aspects of the business have committees to focus on their issues, and risk is no different. For example, all in the business are concerned about the level of sales; the existence of a sales committee to discuss various sales initiatives does not make anyone feel less involved, and the same is true for risk. As is usually the case with committees, a resume of their key actions or decisions, or their minutes, are reported to the main governing body of the division, to ensure that the messages are shared with all.

5.4.2 Within the three lines of defence model, there can be committees at each level, although the committee structure must be proportionate to the particular organisation. Geography is also an issue here.

5.4.3 In the first line of defence, there is nearly always a risk committee. In the insurance environment, this can often be focused only on non-financial risk; typically business, regulatory, and operational risk, on the assumption that the underwriters, finance and actuaries are responsible for the financial risk. Often, this split of responsibilities gives rise to a financial risk committee. In the two committees structure, there is more than sufficient to discuss at each, which many think justifies the split. However, in a future world, where risk is a key metric in the business, and embedding of risk is essential, it will be preferable to have a single unified risk committee as the first line of defence. A division of responsibilities between two committees enforces the view that risk is handled by people in each committee, and is purely a back office function, not mainstream to the business. Another reason given for having two separate committees is that the skill set for each is different, so that this makes best use of resources. Quite clearly there are a wide range of skills necessary to understand, quantify and manage the risks. However, the risk committee should, to an extent, be above this, and be able to receive information from the experts concerning the risks, so that appropriate decisions can be made.

5.4.4 At some time in the future, it is debatable whether there would need to be a separate risk committee. With risk being a key part of the operating model, and being embedded within the business, one challenges the need for a stand-alone risk committee. Even today, where a stand-alone committee exists, often it has a membership very similar to, if not the same as, the executive management of the company. When challenged on why this

is so, the usual response is that it enables the executive to focus on risk, suggesting that it could be seen as an optional add-on. For some companies, this model might be appropriate, the key test is how consistent this approach is with how they review and manage the other aspects of the company.

5.4.5 In the second line of defence, the committee structure will need to take into account the overall Group structure. What is correct for a large multinational Group will, in all probability, be excessive for a small, single country monoline insurer. Assuming there are any, there are generally two types of risk committees at this level.

5.4.6 One type is a committee focusing on the same risk throughout the organisation — thus insurance or credit risk for example. The committee will focus on specifics of the particular risk, will compare appetites between different entities, and will be the primary forum to determine centralised policy management for that risk. This works well in a group with more than one division accepting the risk, and membership is a combination of line one and line two staff.

5.4.7 This committee should also focus on the difference of perception at group and divisional level of a particular risk, and act as the body through which these differences are resolved. These differences have two aspects.

5.4.8 The first is that whilst at a group level there is an overall appetite for this risk, at a divisional level, the local management have a much reduced appetite, often for perfectly rational reasons. As a simple example, consider a composite group writing personal lines household cover. At a group level, there is an appetite for a loss due to adverse weather of £100m. Local management however only have an appetite for £20m., based on their profit targets, and/or the capitalisation of the legal entity through which they write business. This committee should control and co-ordinate the mitigating actions taken to resolve this issue. There are no unique solutions; each group will need to determine what works best, but possible ones include virtual internal/captive reinsurance, external reinsurance, recapitalisation of the divisional legal entity and change of legal entity underwriting the risk.

5.4.9 The second aspect which this committee can co-ordinate, concerns risk diversification benefits allocated at a divisional level. The problem is that with diversification benefits allocated to a particular product or division, the capital utilised is not fully in the control of that division, as the amount of diversification benefit is dependent on risks underwritten by others. Hence this committee can act as the forum through which the overall risks are reviewed, and crucially where all material changes in risk appetite can be considered.

5.4.10 A second type of committee is a subcommittee of the main audit committee, and is often led by the non-executive directors. This focuses on the overall risk management procedures of a particular division. Line two functions as well as the local divisions (line one) would provide input to this committee.

5.4.11 In an environment where the capital in each legal entity is based

in some way or form on its required risk capital, then the linking of the required capital with the actual capital is usually discussed at some form of committee. Risk committees to date have tended to focus on the risks, and not on the sources of capital, and where capital resides. In this case, discussion of the linking of required with actual capital often takes place at a finance committee, with a focus on capital adequacy, or funding and liquidity. However, looking to the future, in particular Solvency II, with approved internal models that require a use test for approval (amongst other things), one can envisage the risk committee will take more control of the linking of required capital with sources of capital, as that will be seen as a more integrated and efficient process.

5.4.12 Appendix B gives a further summary of a possible of governance structure.

5.5 *Risk Management Structure*

5.5.1 There are as many different models for the structure of the risk management function as there are companies. However, there are increasing similarities now being seen.

5.5.2 At the local management level, there is usually a risk team. As has been mentioned earlier, historically this has often focussed primarily on non-financial risk, including operational risk. To an extent, this is a consequence of the evolution of the role. The original risk teams in the U.K. were set up in the late 1980s as compliance teams, to ensure that the rules set by the then regulators for sales methods were in place and were adhered to. There was no obvious need for actuaries to work in these teams. Over time, these teams expanded to be responsible for all aspects of non-financial risk. Meanwhile, the actuaries, particularly under the Appointed Actuary regime, were responsible for the overall solvency of the company. The onset of the ICA regime made this separation less feasible. This, together with an increasing awareness of ERM generally, made it clear that having two separate risk teams was not an optimal way of operating, as each part of the team had a key role to play, and working in isolation was no longer appropriate. These teams focus on risk reporting, and performing oversight activity.

5.5.3 Where a group team exists, it will usually be focused on a particular risk category. In this way, expertise on that risk can be concentrated in a single team at group level, which makes for clarity in knowing who, at group leads on this. It also assists in the overall view of the total risk. The alternative would be a team tracking each division, but this would be inefficient and probably ineffective, particularly in looking at the wider picture, and in setting overall risk management methodologies.

5.6 *Chief Risk Officer (CRO)*

5.6.1 In any structure, there needs to be a head, and we turn now to the role of chief risk officer, which is a key role for the organisation.

5.6.2 It is increasingly common that organisations have their CRO as a member of the executive management. However, the responsibilities allocated to them vary widely. To an extent, this range reflects the different levels of risk awareness and embedding of risk within the organisation. Thus, for a company looking at risk for the first time, and following a traditional financial and non-financial view of the world, the CRO might lead on non-financial risks, with the chief actuary assumed to be responsible for financial risks on the life assurance side and the Underwriting Director responsible for Insurance risks on the general insurance side. At the other end of the scale, companies with a fully embedded ERM process, where risk is embedded in all the key decisions, with associated risk metrics, will have a CRO who has responsibility spanning all aspects of the risk agenda.

5.6.3 The reporting line for the CRO also varies. The most frequent reporting lines for the CRO are the CEO, CFO, or COO. The preferred reporting line is to the CEO, as, in a future where risk is a key aspect of the business, this link makes the importance of the CRO role very clear.

5.6.4 However, there are also many CROs who report to the CFO. There is a rational reason for this, which does not reduce the importance of the role. One of the key metrics in risk is how much risk capital is required for the risk appetite. This amount of risk capital will influence, and in Solvency II 'determine', the amount of regulatory capital required, and hence there is a potential overlap with the CFO, one of whose responsibilities is to manage the overall capital of the company and/or Group. In order to manage this issue, having the CRO report to the CFO enables there to be a clear line of responsibility for matters of capital, both for what is required and what is available. Where the CRO does not report to the CFO, governance needs to ensure that lines of accountability are clear between the two.

5.6.5 Where the CRO reports to the COO, this often is a natural consequence of the CRO being responsible only for the non-financial risks, with someone else, usually finance, actuaries or underwriters being responsible for financial risk. Long term, this looks less likely for many companies, given the need to have a unified view of risk.

5.6.6 As can be seen above, wherever the CRO fits within the organisational structure, there is the challenge of clarifying which executive is responsible for which task. Clearly what is not ideal, is that each executive operates independently of the others, and creates their own infrastructure, and makes decisions based on their view of the world. Besides being inefficient, this duplication can cause material issues when it comes to demonstrating the embedding of risk within the organisation. It is recommended that at an early stage the CRO is made aware of the job descriptions of other appropriate executives, determines what clarifications are required or potential duplications which exist and then discusses any issues with these same colleagues, with a view to ensuring there is clarity on how the risk operating model will operate in the group.

5.6.7 So, what is the skill set required of a CRO?

(a) A solid knowledge of the business, and its underlying risks, both qualitatively and quantitatively.
(b) Communication is key, as much of the value added from the role is derived from explaining to colleagues what the risk agenda is, and how it helps the business.
(c) Having an independent view, and not being afraid to state it. In the 'credit crunch' of 2008, it was clear that there were failings in risk management in many companies. There will, doubtless, have been some risk teams which recognised the issues in advance but were unable or unwilling to get across to others their view of the world, which might have mitigated some of the problems.

5.6.8 Should the CRO be the person who is the expert on financial risk modelling? That skill should not rule out an individual, but many other skills are required in addition to this (in fact, familiarity with financial risk models, rather than expert knowledge, would be sufficient). A possible job description is given in Appendix C. With these comments in mind, where do actuaries fit?

5.7 *Interaction with Actuaries*

5.7.1 Actuaries can, and do, play a key role in performing the detailed calculations underlying the numerical aspects of certain risks. However, whereas in the past they would have been left to get on with this work, and provide information via a few formal processes, for example regulatory reporting and planning, in the modern risk age, they need to involve themselves much more in the wider operation of the company. There is clearly a role for the modelling experts, but to their undoubted technical expertise must be added soft skills, in particular communication, and influencing skills. For insurance companies currently, the actuarial function holder advises the company and its Board on financial risks, and the assumptions thereon. Going forward, one can foresee the CRO being added to this list of people who are advised.

5.7.2 Actuaries do not have an automatic claim on the CRO role. They do have a strong claim to be at the heart of the quantification of risk, and, as such, can contribute much to the risk agenda. With an appropriate range of skills, being an actuary should also not be a negative to becoming the CRO. To an extent, the choice of the individual for the role will be dependent on other factors, including company structure, skills and talents of other senior colleagues, reporting lines and the skill of the actuary in non-financial risk consideration.

5.8 *Internal Audit*

There can often be much confusion between the role of a risk function

and that of internal audit. This confusion arises from the perception (often real) that both teams are playing in the same space, and performing the same tasks. Both groups require clarity about their role, and should understand the other's role. One separation of responsibilities that can work is that internal audit focus primarily on the integrity and control of all processes. Risk functions do not concentrate on process, they focus instead on how the risk is identified and managed. The role of Risk is to ensure that there is some solidity behind the metrics used to assess and manage the risk, and that mitigating actions have been thought through, including the additional risks they might introduce. Internal Audit will review the overall process, accepting it as valid, and give an opinion on its overall control framework and additionally provide assurance that the mitigations relied upon by risk management are functioning and effective, both in normal and stressed conditions.

### 5.9 *Line Management*

Whilst the focus of this section has been on the underlying risk roles and processes, primarily within the risk function or environment, general line management also has a role to play. In addition to adhering to the guidelines and limits given to them, managers need also to understand, and mitigate, where possible, the risks inherent in the operation of their own area. A common way of performing this task is control self assessment (CSA). This is a process where each team works through a controlled set of questions/challenges in order to help it identify its operating risks, and to understand its mitigating actions. When introduced for the first time, there are often initial problems, the primary one being that the exercise is considered to be a box ticking exercise. The risk function and internal audit can work well together in identifying this issue, and assisting in enhancing the quality of the results.

## 6. Implementation — Some Enablers

6.1 Sections 3 and 4 have described why ERM is such a powerful and necessary tool for insurance companies, Appendix A gives a fuller case, and Section 6 has set out some of the key components. This section deals with how to increase the chance of successfully implementing a comprehensive ERM strategy across a company. Some of this is common-sense, but most of it is getting the correct political and cultural environment; actuaries should not underestimate the importance of addressing the cultural side as well as the technical for successful implementation of ERM. However, the most important element of the ERM strategy will be the people driving, supporting and delivering on it within the company.

6.2 Most companies already have in place some, or indeed many, of the

component elements of ERM. That said, an ERM implementation in an existing company of any size will be an extremely large project. It is interesting to note that in the responses to the FSA in the U.K. for the Solvency II QIS 4, those companies which were already well advanced in their overall ERM work believed that they would need more time to deliver Solvency II (which, to all intents and purposes, requires a full ERM regime) than those who were less advanced or had yet to start the journey.

6.3 Any project has more chance of success if those involved have a good picture in their minds of the end result. This is especially true of ERM, which at some level touches almost everyone in the company. Since so few companies actually have fully functioning ERM, and since it is hard to describe in a practical rather than in conceptual way, a vision of the end result can be challenging to determine. The solution, as is often the case, is to break the project into component parts, each of which has a describable and understandable end-point. Success of these sub-projects must be actively celebrated throughout the organisation, and, at each stage, it must be re-emphasised how the components fit into the bigger picture.

6.4 *Sponsorship*

6.4.1 The board are responsible for risk management and internal controls, so ultimately, the drive must come from them. However, the board is formed from a number of individuals, so it is important to get the support of each one of these individuals in order to consider implementing an ERM project. The natural sponsor for a company-wide ERM project is the CEO. The CEO is the most influential executive within the company, and such a high profile sponsor would demonstrate the importance of a properly governed ERM to the rest of the company.

6.4.2 Sponsorship for ERM should be proactive so as to ensure that the company follows the lead. Just implementing an ERM project because it is a regulatory requirement, or because everyone else is believed to be so doing, would limit the added value of the project, and also reduce the likelihood of success. Even if it were successful in delivering the components of ERM, it would probably have minimal impact on the overall management of risk or the achievement of strategic objectives in the company. Although this drive should come from the sponsor, those familiar with risk should also engage and lobby to help increase the chances of successful implementation. Getting support is just the first step in the overall implementation. The sponsor, and other senior management, need to demonstrate their buy-in to the ERM framework, and publicly change their behaviours accordingly. This would send a strong message throughout the company that ERM is an integral part of the strategic management of the company.

6.4.3 The problem is that however much the senior management buy into ERM at an intellectual level, the change in behaviour does not come easily. In the past, when corporate governance was largely implicit rather

than explicit and risk management may not have existed as a separately recognised function, those managers operated with a high level of authority and autonomy. As governance and risk management became explicit, there were inevitably clashes as the new processes acted to constrain that autonomy. Over time this has reduced, as the benefits have become clearer, although there is still a risk that risk management can be seen as slowing down the decision making process.

6.4.4 Strong sponsorship for the ERM project can help to ensure risk management is seen as a benefit by the business and its managers, and indeed as positively helpful to decision making. Risk management successes, where profitable risk opportunities have been actively identified and achieved, can be presented as successes for both ERM and the senior management.

### 6.5 *Value Framework*

6.5.1 A key part of the implementation should be the development of the value framework for ERM. Individuals should be incentivised, usually financially, to achieve their own objectives, which in turn should link to their divisional objectives, which, in turn, should link to the Group objectives. If a measurable statement of risk can be incorporated within these objectives, then it makes the development of a value framework much easier. Once a value framework has been developed, the adoption of good ERM behaviours will become second nature to everyone within the company.

6.5.2 The value framework should be an integral part of the overall strategic plan for the company. This has historically been an issue since planning has typically been tightly defined and resource intensive, which made the inclusion of ERM a challenge. However, if people can see ERM as an explicit component of the company's strategic plan, then it is likely to become more understandable and deliverable by the business.

6.5.3 Any change to the value framework is likely to involve a realignment of individuals' remuneration, and, therefore, it is important to get HR support at the earliest possible stage.

### 6.6 *ERM Implementation Planning*

6.6.1 Once the project sponsor has indicated its support for the project, the next step is to develop a detailed implementation plan. This should be shared with the entire company, and not just be focused on the management of negative risk. It must also comment on the positive impact which it could have for all stakeholders across the company. In a commercial lines GI company, the underwriters are, arguably, the most important stakeholders to be convinced that the project is worthwhile, and that it will have tangible benefits to them upon successful implementation. If they perceive the ERM project as a compliance overhead, and if they cannot be convinced of the benefits of better understanding the holistic company risk, one of the key

holders of risk will not participate actively and many of the benefits of ERM will be lost. Similar comments can be made for life companies.

6.6.2 The issue of project management is outside the scope of this paper, although there is no reason why an ERM implementation project should differ from any other company-wide project in that respect. Indeed, it should deliberately follow the same framework, so that the stakeholders and the resources involved are involved in a process which is already familiar to them.

6.6.3 There are a number of areas of the ERM project which will need to be covered, and these are detailed in the following sections.

### 6.7 *Strategy*

Defining a clear ERM strategy and vision is the key step for successful implementation. It is difficult for people to picture what a successful implementation will look like, and the strategy is there to paint the vision as clearly as possible. It needs to cover an agreed overall value framework for ERM, and should include a discussion of objective setting, and how individuals will be driven to achieve those objectives.

### 6.8 *Governance Committees*

This paper is focused on the governance of the overall ERM framework, and, as part of the ERM implementation, the proper governance to be exercised by the various ERM related committees needs to be documented, agreed and circulated. Clarity over the role of each of these committees will help prevent a duplication of effort, or conflict between the individuals who sit on the committees. Each committee should also have a defined set of responsibilities which they have for executing agreed ERM actions within the company.

### 6.9 *Risk Appetite*

6.9.1 Most companies already have a risk appetite for most or all of their key risks. In the past some companies may have left it at that, but increasingly companies have joined up risk appetites across the different risk types to give an overall company level strategy for the level of risk which it is willing to accept. Without a company-wide view of risk appetite, people will still operate within their silos, and focus on managing the risks which affect their narrow view of the company and which suit their own objectives.

6.9.2 The risk appetite also needs to be split between geographies and operating divisions, so that it can be delivered at every level of the company. Again, this will need to be linked into the value framework to help to achieve a better focus on managing the risks important to the company, rather than just specific to the individual. The value framework should cover how local management performance targets can be adjusted to reflect group

actions and group requirements, otherwise local divisions will feel isolated and alienated from the overall group strategy, and will continue to act in their own interests rather than for the overall benefit of the group.

6.9.3 One approach is to produce an initial statement of risk appetite which captures the current status quo of the firm, particularly if the firm has been successful over recent years. Then, once the firm's understanding of ERM issues improves, an early iteration could examine certain parts of the risk profile more critically or in more detail.

6.9.4 A key issue in getting the acceptance of an ERM framework is deciding on which viewpoint is being used. It is natural in insurance companies, given the close links with the concept of economic capital, for ERM to be designed around the worst case scenarios: (see the right hand side of the graph in Figure 1). It is difficult for management to understand how they should use this 'capital' type view of the world to manage a company day-to-day. This usually manifests itself in an inability to agree to any meaningful expression of risk appetite beyond, for example, 'remain within ICA' or 'maintain current credit rating'.

6.9.5 Senior management is more familiar with managing the company

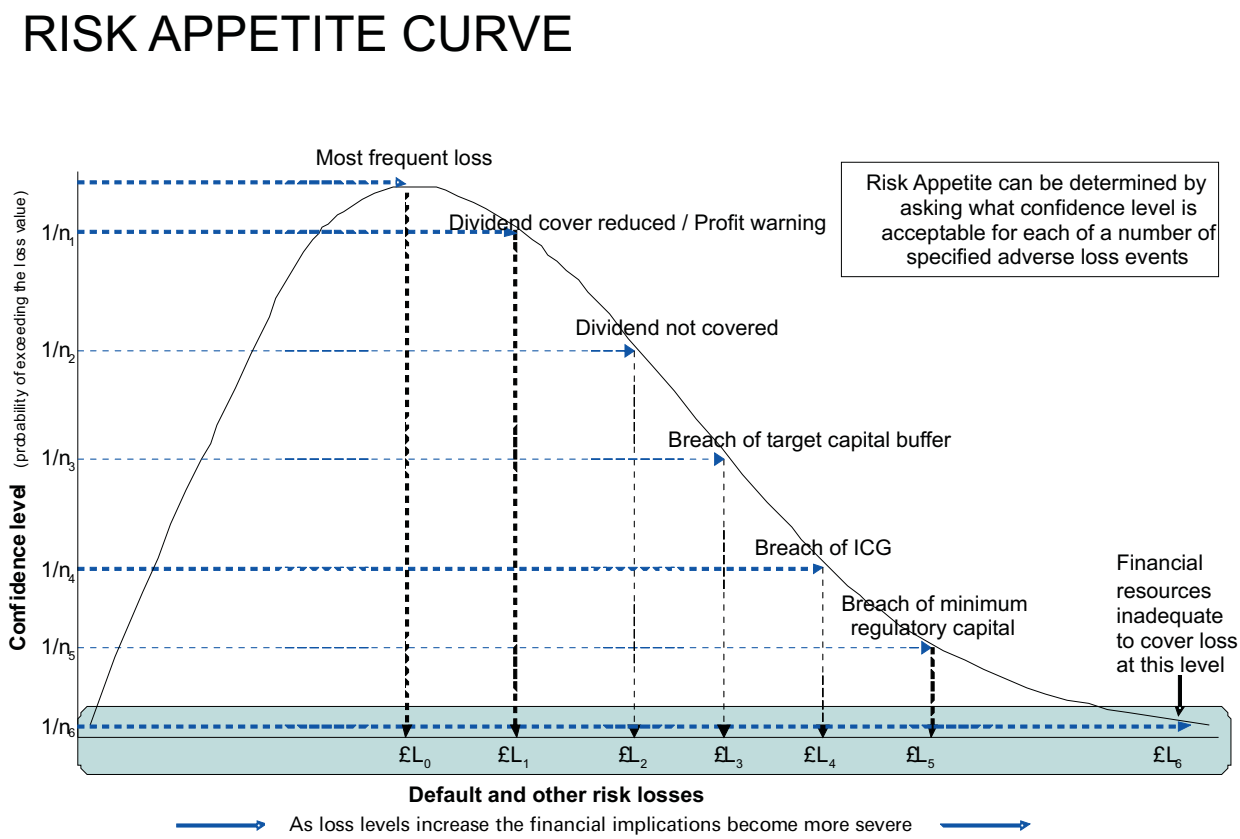


Figure 1. Risk Appetite Curve

to achieve a performance that is within an acceptable tolerance of the business plan, and this should not be surprising, given that this is what drives their remuneration. So, management is more interested in, and perhaps better able to judge, risks around the centre of the distribution than at the extremes. This manifests itself in a ready ability to set a meaningful risk appetite expressed as a variance in earnings, which relates to the central part of Figure 1. That being said, there should be consideration of the economic capital viewpoint when setting the risk appetite since this will capture tail risks that do not feature in the business-as-usual level of losses, and therefore may not have been experienced by the current management team.

6.9.6 Figure 1 represents some of the pressure points that could be identified within a company's risk appetite. The scale is only indicative, although the ordering of the events is correct. Interestingly, any risk appetite would have to note that the underlying model itself may be wrong. For example, a £100m, although modelled as being a 1 in 50 year loss, may in reality have a much higher or lower probability.

### 6.10 *ERM Execution*

6.10.1 ERM covers identifying, controlling and monitoring risk, and therefore there needs to be detail about how management action will be taken when risk appetites are exceeded, or are close to being exceeded. The onus on execution is with the ultimate risk owner, although CEOs have a strong vested interest, given their requirement to consider risk across the whole of their companies. An example of this is that there should be an execution strategy to rebalance equity exposures across the group, in order to maintain local solvency, and this strategy should be ideally defined before equity markets fall, and such action becomes a requirement as opposed to a potential issue.

6.10.2 ERM is likely to change some of the roles and responsibilities for individuals. Depending on the scale of change, some internal reporting lines may need to change so that the manager for an individual has a strong vested interest in their charge successfully achieving their objectives.

6.10.3 The reporting lines for the ERM team should also be made very clear, since this will then give clarity to the business as to who is responsible for what, and how to escalate any risk issues, if necessary.

### 6.11 *Creating the Right Environment*

6.11.1 There must be a genuine acceptance of joint responsibility between non-executive and executive directors. This is crucial, because without an open environment where the giving and the receiving of news, especially bad news, is not properly accepted, ERM cannot be implemented successfully. The executives need to cascade this message throughout the company, and demonstrate clear evidence to staff that the messenger of bad

news will not be shot (unless, of course, the bad news was foreseeable, they were the responsible party, and they deliberately did not take any mitigating action).

6.11.2 Where someone has demonstrated that the ERM process successfully helped them in some way, then this could usefully be publicised across the company. Creating such 'risk heroes' may mean celebrating near misses. This might run counter to the previous culture but would increase the profile of ERM by making people more aware that their actions are positively recognised by senior management.

6.11.3 Where there is good news, this should also be shared across the company. If there are 'quick wins' which can be achieved, then the likelihood of a successful implementation will increase, since people will have a better grip on the cost/benefit of the project. Examples of such wins which have been experienced in the past are:

(a) Evidence that linking two controls in different areas had allowed a third, unwieldy, control to be scrapped.
(b) By considering risk from a top-down basis, more efficient reinsurance programmes can be structured without exceeding underwriting risk limits. This is particularly the case for groups where historically, divisions have tended to purchase reinsurance to manage their divisional level risk without considering the link to the overall group risk appetite.
(c) Identifying future emerging risks can enable GI underwriters to price a particular risk better, and/or to include exclusions to mitigate the potential for the emerging risk to become an actual liability to the company.

6.11.4 If the tone from the top is correct, and people can see where the project is going, then they are likely to get behind it, and to live and breathe ERM values. However, for this to happen, they need to see that their managers at all levels up to the top of the company, are actually doing something different.

### 6.12 *Communications Strategy*

The ERM implementation plan should have a detailed section on project communications, which should cover communication within the team, communication with ERM stakeholders, high level communication to the entire business, and also external communication with regulators and rating agencies. A clear and cohesive communications strategy is the first step in engaging the hearts and minds of the individuals within the company, and such engagement is necessary to ensure that everyone is considering risk in their day-to-day activities. Given the importance of the communications strategy to the implementation of ERM, it is discussed in more detail in the following section.

6.13 *ERM and PR*

6.13.1 It is a relatively easy job, at a high level to describe the concepts of risk management and ERM. It is also relatively easy to describe, and even to implement some of the components described in Sections 4 and 5. For it to succeed, it is essential to win the 'hearts and minds' of the rank and file staff. This is because they are the ones often closest to the detailed things which can go wrong, and they are also the ones likely to be operating the internal controls. A control which is not taken seriously has a significant chance of malfunctioning or not being operated at all. Also, without the hearts and minds, the risk function could be perceived as an overhead with nothing to bring to the business.

6.13.2 As with many things, this means dealing with questions like: "Isn't this just more work for me?" and "What's in it for me?" At the more junior levels it is unlikely that this can be addressed by remuneration since it is primarily a PR problem.

6.13.3 For middle to senior staff, behaviours can, to some extent, be modified via remuneration design: "What get's measured get's done". However, relying solely on this can be dangerous, since people can be ingenious at manipulating remuneration systems without actually achieving what the designers intended. So, again, PR has a large role to play at this level too.

6.13.4 A big problem here is that it is very difficult to look outside the company to point to examples of: "Look at the good things that ERM did for them". This is because the PR does not work in the other companies either, or the other company jealously guards its risk management successes as it views them as a competitive advantage. It also does not help that, when a company does well, it is as a result of '*the drive and strategic vision of our underwriters and key executives*'. When a company does poorly and has unanticipated losses, or collapses completely, it is sometimes attributed to 'risk management did not operate as anticipated on this particular occasion', with little mention of the actual offending parties. This means that the main PR for ERM relates to the avoidance of risk, which is not an easy message to sell in a culture which, traditionally, celebrates revenue generators.

6.13.5 Note that we are not suggesting that ERM should focus on completely avoiding any risk within the organisation, since it is risk which gets rewarded in an insurance company. Accepting anticipated risk losses is acceptable subject to the appropriate control framework. ERM should be there to help to accept risk in a controlled fashion, and to understand the risks which are being run, in order to reduce unanticipated risk losses. ERM is as much about the reward as the risk, and the question is about whether the reward justifies the risk, rather than avoiding the risk in the first place.

6.13.6 There are a number of PR issues, some of which are easier to address than others. For example, although it is relatively easy to describe

the concept and the components of ERM, it is far from easy to describe to someone what ERM 'feels' like when it is working properly. How can it be distinguished from the current situation? What do we do differently? In reality, few people can actually describe an internal control. A positive view of risk ought to help here, since describing ERM as a way of avoiding lost opportunities sounds good.

6.13.7 One way of assisting in the PR effort is to have a functioning set of risk committees at the non-executive director level, allied to a strong independent risk function. This will ensure that comments made on risk management are credible and treated seriously.

6.13.8 If staff and line management have not truly bought into the ERM concept, there is a danger of avoidance which must be addressed. In other words, risk management activity gets relegated to the end of people's to-do list. Symptoms will be risk reports which do not change from period to period, no reporting of loss events or near misses, and ultimately control failures. Such behaviour is not conducive to personal ERM, let alone company-wide ERM.

6.14 *Training*

6.14.1 There is a significant amount of training which should be covered as part of the ERM implementation plan.

6.14.2 Boards may need to be educated on their roles and responsibilities as part of the overall ERM strategy, and also possibly to be educated on ERM related outputs (such as the output from the economic capital model). The latter of these two has developed significantly in the U.K. over the past five years, although there is probably still further progress to be made.

6.14.3 Divisional management boards may need education on how the risk appetite has been split across the group, and what is expected of them in terms of local risk oversight, and how their management results are to be adjusted for group requirements.

6.14.4 ERM resources may need additional training. For example:

(a) Actuarial staff are likely to require an amount of re-training on how to cover some of the softer aspects of risk management, as well as getting up to speed on some of the more technical topics such as credit risk.
(b) The existing risk management department, who may have been largely focussed on managing qualitative and non financial risk in the past, may require some training on quantifying risk and how the economic capital model works.

6.14.5 Other staff will need to be educated on their responsibilities under the ERM framework, and what is expected of them. This education should also cover the benefits of having ERM, as this will help to increase the chances of a successful ERM implementation.

6.15 *Economic Capital Model and other Metrics*

6.15.1 A key component of ERM should be a robust economic capital model, as well as other quantitative metrics that help identify risk within a company. This is not a model in the typical sense that it is a stand-alone piece of coding with a 'run' button, but more a process to take the risks inherent within the business and translate them into a financial amount. This could include a large element of quantitative analysis (such as the stochastic modelling of asset and liability cash-flows), but is also likely to incorporate qualitative judgement of some of the risks that cannot be modelled easily numerically. Whatever the overall framework of the economic capital model, it needs to be sufficiently industrialised so that economic capital numbers are both accurate and timely.

6.15.2 The outputs from the model should be regularly reported and discussed at the appropriate committee, and should additionally be formally presented to the board throughout the year. Analysis of change and the explanation of variances can be very informative in helping the board to understand the key risks of the firm. Other risk metrics, e.g. staff turnover rates and current lapse levels, should also be presented as part of these discussions. The combined outputs should distil the key risk indicators across the business, and show how ERM is assisting the management of them. It should also consider 'ripple effects' across different risks, although this does not necessarily mean that complicated correlation matrices and dependencies are required. Ideally a risk dashboard should be developed as part of the ERM implementation plan which will inform senior management and the board at a glance, as to the overall risk profile of the company. Such a tool could then be used to monitor the risk within the business, which is one of the key requirements for a successful ERM implementation. It also allows the board, if necessary, to redirect the focus of the line and/or the risk management activity for the next period.

6.16 *External Assurance*

6.16.1 External assurance of the ERM strategy and implementation plan will help to provide the ERM stakeholders with comfort that the approach is fit for purpose. Although external consultancies do not have the specific knowledge of the company which is required to implement ERM properly, they do have the breadth of knowledge across companies that will inform where strengths and weaknesses lie within the strategy. The remit for this assurance review should be relatively broad in order to maximise the value of the reported feedback to the readers.

6.16.2 It is also very likely that external assurance would be considered desirable on the economic capital model, which is large, complex and sits at the very heart of the ECM value framework. In fact, it is likely that this will actually become a regulatory requirement in the future.

## 7. Implementation — Some Barriers to Success

7.1 Given the obvious benefits of a quality ERM framework, and the pressures from external bodies, such as the FSA and ratings agencies, why is it that U.K. insurers are not much further advanced with their ERM frameworks? By the end of 2007, only 3% of the 274 worldwide companies reviewed by Standard and Poor's had achieved their highest ERM rating of 'excellent'. The reason for this is that ERM is more than a set of simple mechanical processes, and that it requires a significant change in a company's approach to management and in its culture, both of which are potentially material barriers to implementation.

### 7.2 *Executive versus Non-executive Directors*

7.2.1 In the Introduction and Section 4 we discussed the agency problem between the owners of a company and its management, and expanded this to two levels: shareholders versus board and board versus management. The second of these, the difference of interests between executive and non-executive directors, is a potential barrier to successful ERM implementation.

7.2.2 For executive directors and other senior management, the job is their primary source of current and future income, and also their primary route for future advancement (they may, of course, leave the company for a better job, but the likelihood of getting one will depend highly on their reputation for performance and delivery at the existing job).

7.2.3 Non-executive board members monitor and, if necessary, control the executive directors and senior management. With the possible exception of the chairman, they are less concerned with their current and future income from the company, but are more concerned about its proper running. Indeed, they typically receive lower levels of remuneration for their roles, since, otherwise, they could not be deemed to pass the 'independence' requirement of the role.

7.2.4 Through remuneration and nomination committees, non-executive directors control the pay and the advancement of executive directors, and, in many companies, a number of layers below this level as well. Therefore, there is a natural tendency for managers to want to create a consistently good impression in front of the board, which could develop into a continuous process of self-publicity about the quality of their work and their achievements, and place less emphasis on the failures and the risks they for which were responsible. In these circumstances, the non-executive directors would not receive a neutral, unbiased flow of news, and this is not conducive to a good ERM framework in a company.

### 7.3 *Risk Management versus Line Management*

7.3.1 What exactly constitutes a risk management function, and what is its role? There are a number of models, but most would recognise that, in the

first instance, risk management is the responsibility of line management. This is entirely consistent with the idea of risk management being embedded within the business. It also emphasises the way in which ERM must be built into the cycle of identifying and achieving objectives. Where it can be harmful to ERM is where the result is 'silo' based risk management, with no communication or co-operation between silos.

7.3.2 Whilst line management at the operational level might, therefore, deem risk management to be just one of its roles (alongside operations, HR, etc.), it is increasingly common for line management at this level to create its own risk management team. This has the advantage of providing focus and capacity, but has two problems:

(a) The first is defining clearly the roles of operational and risk staff, and 'spreading the gospel' of risk management benefits so that operational managers do not see the risk team as a nuisance and an overhead.
(b) It raises the question of to whom the risk team at the operational level reports. Is it to line management at that level or the next, or upwards, via separate risk management reporting lines?

7.3.3 This reporting issue has already been discussed in detail in section 6, so is not covered any further here. Linked to this is the question of career progression. Without its own reporting lines, there may seem few opportunities for promotion for risk staff, and this may affect the quality of staff prepared to enter risk management. This is analogous to the problems which internal audit teams have had with recruitment and retention over the years. In many companies, the view is that this has been solved by developing rotational plans, promoting internal audit as a fast track training ground, providing high flyers with a wide ranging view of how a company operates, and then ensuring internal auditors return into well regarded jobs. Whilst some of these concepts could be applied in risk management, a key difference is that the majority of accountants have some audit experience in their background and can slot into internal audit quickly, with relatively little company or personal investment, then return to use those and other skills elsewhere just as easily. Risk management skills and training are, at present, much rarer. Trained risk managers can be difficult and expensive to recruit, and so the company is likely to want to keep them in the risk function. If other professional staff are persuaded to join risk management, it is also likely to be seen on both sides as a much longer term investment.

7.3.4 A negative view of risk management may also a barrier to entry and retention. The perception that it is either preventing potential developments in a company, or failing to spot risks of which the rest of the business was unaware, could make the role unpopular. To some extent, the solution to this is in the hands of the risk management team, but senior management must support the recognition of the risk management contribution within their company, in order to keep the right people working there. Another solution

is to make it a central and visible role of the risk management team to drive the understanding of return on capital or the quantification of economic value added into the front line departments of the business.

7.4 *Theory versus Practice*

7.4.1 As mentioned in the introduction, risk management has developed to a sophisticated level in the banking world. This development has run alongside the development of the derivatives markets, and both have been populated by a large number of extremely well qualified 'quant' specialists. Based on a few key theories and assumptions of financial economics, an entire edifice has been created using tools from mathematics and the physical sciences. Central to this is the view of 'risk' as synonymous with volatility. Originally applied in relation to asset prices, this approach has been extended to other forms of risk within banks.

7.4.2 Despite the overwhelming support for this view, there have always been some who argued that this misses the point in a number of ways:

(a) It has become too divorced from the day-to-day concept of risk that it is 'the chance of things happening that might hurt us'. This concept is not expressed in mathematics, but is pretty well understood by all.
(b) The theories and assumptions that are the foundations of the edifice are simply that, theories and assumptions, and they may not be valid. For example, there is plenty of evidence to suggest that markets are not efficient. Similarly, events of the 2008/2009 in both equity and credit markets seriously question the assumptions of continuous movements and the normal distribution.
(c) Mathematics cannot answer some of the risk questions raised by the board. For example VaR would only give a partial answer to the question of launching a product, since it does not cover risks such as reputational risk.

7.4.3 Put these two together, and, with the benefit of some pretty fresh hindsight, we can see that it would be easy to fall into the trap of serious over-reliance on a framework which is intellectually tempting but fundamentally unsound. Against this background, should we be concerned that the FSA has based the regulatory system for insurers on essentially this same framework, and Europe is about to follow in their footsteps with Solvency II?

7.4.4 We are not suggesting that existing risk management approaches should be rejected. Although potentially flawed, existing risk approaches are still better than what went before. The mathematical approaches do allow us to understand and express issues in a way that words cannot, and they need to be used going forward with an explicit acknowledgement that they do not represent reality.

7.4.5 This dichotomy of being skilled in, and comfortable with, complex models, whilst at the same time being wary of placing complete reliance on

them in decision making, is something which the actuarial profession understands very well. We must continue to stress this point in our education system and in promoting the profession. We must ensure that the users of our advice in the risk arena understand its limitations when based on modelled results.

7.4.6 In practice, we need to blend the models with insights from the 'human' view of risk. We need to worry about the things which can hurt us even if the model says that they will not happen, and this makes judgemental expert input to the model invaluable.

### 7.5 *Relationships with the FSA and Ratings Agencies*

7.5.1 Companies should build ERM frameworks, because they believe in them and in the benefits which they bring. Unfortunately, this is not always the case, and sometimes it is done because the regulator and/or the ratings agencies say that it should, but this attitude is likely to cause a well thought-out ERM framework to at best, falter, and at worst, fail. However, the impact of these relationships are important to ERM, since, ultimately, the FSA and the rating agencies are two of the key external stakeholders in any company.

7.5.2 To get some of the financial benefits (e.g. credit in the ICG, or an improving rating/avoiding a downgrade) from these two external parties requires early, regular and open dialogue. Due to a company's investment in ERM, there is a desire by management to present their ERM frameworks in the most positive light possible, and this may include suggesting that some of the planned developments are already implemented and are up and running. Such obfuscation over ERM will quickly be seen through since the FSA and the rating agencies have developed their staff internally and have completed numerous on-site ERM appraisals. They can also use internal and external audit reports on the effectiveness of the risk management function in assessing the quality of the framework and its implementation.

## 8. Conclusion

8.1 Historically, many actuaries within insurance companies would have considered themselves actively involved in risk management, without necessarily using the term. It would therefore seem natural for actuaries to form the core of any newly established risk management function in an insurer, and to be flag carriers for the introduction of enterprise risk management. Actuaries would also like to be considered well suited for the role in other industries.

8.2 The paper has painted a picture of the wider Enterprise Risk Management arena, and shown that there is much more to this than simply computational models — although clearly the information provided by these

remains a key factor. One of the challenges of the subject is that it is still in its infancy, and there is no standard template that works for all companies. Each organisation will need to implement what works for it, taking account of its particular operating model. Both as a consequence of normal evolutionary development, and the onset of Solvency II with its proposed use test, there will be much progress in the next few years, which should lead to a more clearly defined regime. However, risk will always retain its subjective element.

8.3 However, there are some constants in successful implementation. The predominant one, based on the authors' practical experience, is that the cultural aspects of implementation, in particular getting non-believers to believe and getting believers to be seen to behave as such, is key to achieving ultimate success. We hope that the ideas and information contained in this paper can form a useful aid to implementation.

## Acknowledgements

Various members of the ERM Practice Executive Committee have commented on drafts of this paper and we thank them for their input. However the views and opinions expressed, and any remaining inaccuracies, remain the responsibility of the authors.

This paper would not have seen the light of day without the significant assistance of Maria Austin, to whom we also extend our thanks.

## References

A.M. Best Company. *Risk Management and Rating Process for Insurance Companies.* Available at: http://www.ambest.com/ratings/process/ratingprocess.asp

Cadbury, A. (Chairman) (1992). Report of the Committee on the Financial Aspects of Corporate Governance. Available at: www.ecgi.org/codes/documents/cadbury.pdf

CFO Forum (2008). *Market Consistent Embedded Values (MCEV): Principles and Guidance.*

CEIOPS Quantitative Impact Studies. Available at: http://www.ceiops.eu/content/view/118/124/

Committee of Sponsoring Organisations of the Treadway Commission (2004). *Enterprise Risk Management: Integrated Framework.*

The Companies Act (2006). Available at: http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060046_en.pdf

The Company Directors Disqualification Act (1986).

Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance. Available at: http://eur-lex.europa.eu/LexUriServ.do?uri=OJ:L:2002:077:0022:en.pdf

Directive 2002/13/EC of the European Parliament and of the Council of 5 March 2002. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:0077:0017:0022:en.pdf

European Commission (2008). *Directive of the European Parliament and of the Council on the taking up and pursuit of the business of insurance and reinsurance (''solvency II'').* Available at: http://ec.europa.eu/internal_market/insurance/docs/solvency/proposal_en.pdf

The Financial Reporting Council (2005). Internal Control: Guidance for Directors on the Combined Code.
http://www.frc.org.uk/documents/pagemanager/frc/Revised%20Turnbull%20Guidance%20October%202005.pdf

The Financial Reporting Council (2008). The Combined Code on Corporate Governance.
http://www.frc.org.uk/documents/pagemanager/frc/Combined_Code_June_2008/Combined%20Code%20Web%20Optimized%20June%202008(2).pdf

The Financial Services and Markets Act (2000).

The Financial Services Authority (FSA) Handbook. Available at:
http://fsahandbook.info/FSA/index.jsp

The Financial Services Authority (2008). Discussion Paper: Insurance Risk Management: The Path to Solvency II. Available at: http://www.fsa.gov.uk/pages/Library/Policy/DP/2008/08_04.shtml

Higgs (2003). Review of the role and effectiveness of non-executive directors. Available at: www.berr.gov.uk/files/file23012.pdf

The International Accounting Standards Board (2008). *IFRS 4*. Available at:
http://www.iasb.org/IFRS+Summaries/IFRS+and+IAS+Summaries+English+2008/IFRS+andIAS+Summaries+English+htm

IT Governance Institute. Control Objectives for Information and Related Technology (COBIT). Available at: www.itgi.org

Public Company Accounting Reform and Investor Protection Act (2002). Available at:
http://thomas.loc.gov/cgi-bin/query/z?c107:h5070:

Smith (2005) Guidance on Audit Committees available at: http://www.frc.org.uk/documents/pagemanager/frc/Smith_Guidance/Smith%20Report%202005.pdf

Standard & Poor's (2006). Refining the Focus of Insurer Enterprise Risk Management Criteria. http://www2.standardandpoors.com (this one is not freely available).

Standard & Poor's (2008). Enterprise Risk Management: ERM Development in the Insurance Sector could gain strength in 2008. http://www2.standardandpoors.com/portal/site/sp/en/us/page.article/2,1,6,4,1204834496637.html

Turnbull, N. (Chairman) (1999). *Internal Control: Guidance for Directors on the Combined Code*. London Stock Exchange.

Lord Turner, Chairman FSA (2009). Speech made at The Economist's Inaugural City Lecture 21 January 2009. Available at:
http://www.fsa.gov.uk/pages/Library/Communication/Speeches/2009/0121_at.shtml

Tyson (2003) Report on the Recruitment and Development of Non-executive Directors. Available at:
http://www.london.edu/facultyandresearch/research/docs/TysonReport.pdf

# APPENDIX A

## WHY UNDERTAKE AN ERM PROGRAMME?

A.1.1 If one undertakes an internet search via a search engine, there are numerous papers available which extol the virtues of ERM. At a high level they simplify to a definition of

> The process of planning, organising, leading and controlling the activities of an organisation in order to minimise the effects of risk on an organisation's capital and earnings.

A.1.2 A more detailed and fuller summary, is contained in a paper entitled 'Enterprise Risk Management: Integrated Framework' produced by the Committee of Sponsoring Organisations of the Treadway Commission in 2004.
(http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf)

The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept, as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to deal with uncertainty and associated risk and opportunity effectively, enhancing the capacity to build value.

Value is maximised when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives. Enterprise risk management encompasses:

- *Aligning risk appetite and strategy* — Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- *Enhancing risk response decisions* — Enterprise risk management provides the rigor to identify and select among alternative risk responses — risk avoidance, reduction, sharing, and acceptance.
- *Reducing operational surprises and losses* — Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- *Identifying and managing multiple and cross-enterprise risks* — Every enterprise faces a myriad of risks affecting different parts of the organisation, and enterprise risk management facilitates

effective response to the interrelated impacts, and integrated responses to multiple risks.

- *Seizing opportunities* — By considering a full range of potential events, management is positioned to identify and proactively realise opportunities.
- *Improving deployment of capital* — Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

These capabilities inherent in enterprise risk management help management achieve the entity's performance and profitability targets and prevent loss of resources. Enterprise risk management helps to ensure effective reporting and compliance with laws and regulations, and helps to avoid damage to the entity's reputation and associated consequences. In sum, enterprise risk management helps an entity to get to where it wants to go, and to avoid pitfalls and surprises along the way.

# APPENDIX B

## A POSSIBLE GOVERNANCE STRUCTURE

B.1. There are many differing ways in which to construct a risk governance infrastructure. This is a fairly generic example. It is based on a large corporation, but something similar could be used for a much smaller and simpler corporation. The key point to note is that, no matter what the size of the group (or even a single company) the governance included here should be appropriately covered.

B.2 The group consists of stand-alone legal entities in a variety of E.U. and non E.U. countries, offering some or all of life assurance and general insurance (GI), asset management, banking and insurance broking. Each country is run with a combined management, but with separate legal entities for each activity.

B.3 Opinions vary on what role a committee (in general, not specifically risk) should perform. One view is that the committee has primary oversight responsibility, but, in order to ensure the smooth running of the overall operation, individuals have delegated authority for a majority of the key issues. In this case, the committee will act as a forum, whereby the past and the upcoming issues are discussed and reviewed. An alternative view is that the authority is with the committee, and not with individuals. In this case, the committee will need to meet frequently, and members will have collective responsibility for decisions. Clearly, within a group, both types of committee can exist, and indeed, varieties in between, but all involved should be very aware of the role and the responsibility of each committee, which should be documented.

B.4 *Level 1 Governance*

B.4.1 Level 1 Governance (local country/division level):

(a) legal entity boards, with non-executive and executive members;
(b) divisional/country risk committee — This committee is usually comprised of executives, but could include non-executives. A key consideration in whether to include non executives is the extent of their involvement at another level of governance;
(c) local audit committee; and
(d) country executive committee.

B.4.2 Membership of all the above is predominantly local country, with some group representation. Where there is group representation it is often, but not always, via the appropriate group risk personnel. The group representatives would effectively act as if they were non-executive directors in relation to the local business.

B.4.3 These committees do not report to the Level 2 committees, although

to facilitate linkage between the levels, the Level 1 committee will provide a summary of the key issues to the appropriate Level 2 committee. This could be a nil report; it is definitely not the meeting minutes or the outstanding actions list.

B.5 *Level 2 Governance*

B.5.1 Level 2 Governance (Group oversight and control):

(a) group insurance risk committee, responsible for all aspects of insurance risk. This would typically be separate for life and GI risks;
(b) group market and credit risk committee, responsible for all aspects of market and credit risk;
(c) group capital committee, responsible for consolidated risk capital, and its control. This can often be led by group finance, as it is concerned with overall capital for the group, and included in this could be funding and liquidity, but this could also be a stand-alone committee. This could consider the aggregation of risks, and the allocation of capital to each;
(d) group asset and liability committee (commonly known as GALCO), which can include aspects of market risk, capital and liquidity;
(e) group operational risk committee, responsible for the non-financial risks of all types and for the internal control framework. Strategic risk can also be considered here; and
(f) membership is usually a combination of the group and a representative from each local country/division. There is not usually any non-executive representation in this level of committees.

B.6 *Level 3 Governance*

B.6.1 Level 3 Governance (assurance to Group):

(a) group audit committee, with sub-committees covering risk. These sub-committees can focus either on risk type, and thus are parallel to the level 2 committees above, or more usually focus on each country or division. In addition to risk responsibilities, these committees would usually be responsible for providing the annual sign-off required under Turnbull (1999).
(b) Membership is only non-executive directors, but with group functions and key divisional personnel attending and presenting papers.

## APPENDIX C

## JOB DESCRIPTION FOR A CHIEF RISK OFFICER

C.1 *Core Purpose of Role:*

(a) To support effective, efficient and consistent execution of divisional (group) strategy, compliant with the group's risk appetites and policies; or

(b) to lead, develop and maintain the capabilities within (group) risk (and across the group) to support the achievement of the risk vision and strategic objectives with regard to the risk framework.

C.2 *Accountabilities:*

(a) To provide analysis and insights which enable risk/reward trade-off to be optimised and to plan for an appropriate range of upside and downside scenarios.

(b) To establish a control framework, governance structures, culture, oversight and monitoring arrangements which ensure compliance with the risk framework.

(c) To provide independent oversight and assurance of the effectiveness of risk management and to provide assurance on this to the group board.

(d) To provide accurate, timely and actionable reporting.

(e) To establish and maintain the group's ability to quantify its economic capital requirements on both regulatory and internal bases.

(f) To ensure group policy statements are appropriate, regularly reviewed to reflect internal and external changes, and effectively communicated.

(g) To provide line management for the group risk team and functional leadership for personnel in the wider risk community. To ensure appropriate risk management within the risk management function itself.

(h) To provide input into research capability to ensure the group is kept abreast of the latest risk developments and harness such development for the group.

Printed by Bell & Bain Ltd., Glasgow