RISK MANAGEMENT & CORPORATE GOVERNANCE

By Richard Anderson & Associates

This report was prepared for the OECD by R. C. Anderson (rc.anderson@tiscali.co.uk).

I Executive summary

101 This paper portrays a picture of Corporate Governance in The United Kingdom, the United States of America and France in the banking sector being severely challenged in an extreme Financial Crisis that has seen household banking names run into trouble, some to fail and others to be taken into various degrees of national ownership. Corporate Governance is stretched to the extent that it is distressed and has been unable to cope with the demands placed on it. The rationale for saying that it is stretched is as follows:

- Corporate Governance is (almost) voluntary;
- Investor pressures are fierce, leading many businesses to undertake risks that simply are not in the best long term interests of the organisation;
- Non-executive oversight is stretched in that directors only have a limited amount of time to devote to the organisation, but almost unlimited responsibilities;
- External audit is stretched to a point where the degree of reliance that is placed upon it is out of proportion to the amount of work that actually goes into it;
- Internal audit is struggling, largely because many internal auditors are not the beneficiaries of the regard that they are owed;
- Obtaining assurance from regulators, financial analysts and rating agencies cannot be comprehensive;
- Which leaves boards with dependence on management including the risk management team, and General Counsel (or the Company Secretary).

102 It is a conclusion of this paper that Corporate Governance alone is not the cause of the current Financial Crisis. However, Corporate Governance could have prevented some of the worst aspects of the crisis had effective governance operated throughout the period of time during which the problems were developing and before they crystallised. Furthermore, effective Corporate Governance could have helped to reduce the catastrophic impacts that the global and national economies are now suffering.

103 The main finding of this paper is that the balance between risk-taking (the life blood of the free market) and risk avoidance is no longer functioning. Similarly, the balance between remuneration (one of the principal drivers of the performance culture in the banking sector) and ethical behaviours no longer operates appropriately. The oversight over these two principal balancing acts, which should be exercised by the board, and in particular by the non-executive or independent directors does not function properly because the assurance functions are not given sufficient weight. Therefore as a matter of policy, in order to meet the needs of society, there is a need for a significant rebalancing of boards and assurance functions in companies that are of societal importance, such as major banks. Oversight by non-executive directors is sometimes too remote and distant and it is difficult, in global, complex organisations for this to be discharged effectively by part-time non-executive directors. Accordingly policy makers should consider whether more emphasis should be given to oversight by both the creation of full-time non-executive directors and the development of a broader concept of assurance.

104 While the focus of this paper has been on the financial services sector, and particularly on banks, many of the recommendations would equally be valid to other organisations which have a major societal impact, including for example corporations that play a major part in the critical

national and international infrastructure of the national and global economies. The re-balancing of responsibilities would help to ensure that such organisations remain focused on the needs of society as a whole rather than simply on the investor and executive management interests.

105 In broad terms this paper proposes innovative new mechanisms that can enable bank (and other) boards to discharge their Corporate Governance responsibilities with the required due and diligent care. The ultimate purpose of these new mechanisms is a change of culture in the board room, especially in the banking industry, which in essence underwrites the entirety of our economic system. To support this innovation, the paper also advocates the professionalization of management in the banking sector by means of the creation of an international professional management association.

106 In writing this paper it has become clear that none of the existing guidance on risk management is adequate for the purpose. Most of the guidance is extremely high level, is process-oriented and gives scant guidance on how to create an effective risk management and assurance framework. The paper advocates a balanced approach to risk management that addresses the pitfalls and the ethics as much as the risk taking and the performance culture; that encompasses the totality of the risk universe, both within the organisational boundaries and across semi-permeable boundaries into the extended enterprise. The paper encourages boards to assess and manage the risk management culture, risk management maturity and it stresses the overall importance of ethics to the management of risk. The paper encourages boards to take a more pro-active stance in overseeing the risk management framework as part of the development of the assurance framework.

107 In order to compensate for the extreme pressures for growth that have been so evident in the banking sector and also to compensate for the distressed state of Corporate Governance, this paper advocates a significant increase in the board's oversight of assurance across the organisation. This would address the risk management group, the internal audit department and other internal assurance providers. Boards are encouraged to consider the appointment of a senior Chief Assurance Officer, or Director of Risk Management and Assurance to pull the whole picture together. Boards are also encouraged to consider the appointment of full time directors whose main responsibility is to ensure that sufficient attention is paid to the risk management and assurance framework, especially where there are significant societal responsibilities. Finally the paper advocates that boards should commission independent governance audits.

108 All of the recommendations made in the report are included in the following table:

109 It will not be a surprise that some banks are doing some of the things that are being recommended in this paper. It is unlikely that any bank will be doing all of them. The overall message is that there are some things that they could do now, some require policy makers to review the structure, balance and objectives of boards (for example heightening the important of assurance) and some require the banking regulators and supervisors, and the organisations that maintain codes of corporate governance either nationally or internationally to conduct further work. Some of the recommendations can be implemented rapidly and some will require a period of years for implementation.

110 Taken together, the recommendations in this paper would reinforce the overall system of Corporate Governance, provide reassurance to external stakeholders, including society as customers and as taxpayers, while ensuring that the entrepreneurial spirit of the banks (and other commercial organisations) and the scope for innovation is not restricted, but simply subject to a healthy degree of oversight by independent non executive directors and properly constituted, managed and funded assurance functions.

II Background

202 The Financial Crisis needs no introduction in this paper. The scale of the collapses across the globe and the ramifications for the rest of the global economy are well documented in many other places. The question that the cumulative collapse of shareholder value around the world begs is whether the failure is one of Corporate Governance or not. This is not simply a semantic question: following the examples of Enron, WorldCom and others in the United States, the Sarbanes-Oxley Act introduced some major changes to US Corporate Governance. On the other hand, in response to more isolated examples elsewhere, such as the collapse of Marconi in 2001 in the UK, leading commentators argued that this should not be seen as a failure of Corporate Governance since the failure was principally due to a misguided strategy, rather than a collective board failure. Following this logic, one might well argue that the Financial Crisis was not so much a failure of Corporate Governance but rather a "Perfect Storm" within the global banking industry, which boards could neither be expected to foresee or to react to swiftly enough to make a substantial difference.

203 Such arguments, which are normally made in order to rebut the need for change in Corporate Governance arrangements, may be misplaced in that they can lead to missed opportunities for reform. Hence the failure in the UK in the wake of Enron and other scandals to reform the UK Corporate Governance arrangements, in no small part due to an "establishment" view, expressed by many that "it [failure on such a massive scale] could not happen over here". "It" (a massive failure on a massive scale) clearly has happened over here and it is incumbent on us to look at all of the contributing factors which either caused the problems or prevented them from being managed in as effective manner as possible, right round the global economy.

204 With this in mind, it is helpful to recall the purposes of Corporate Governance. The Financial Reporting Council (FRC) Combined Code sets out the purpose of Corporate Governance as follows:

> "Good corporate governance should contribute to better company performance by helping a board discharge its duties in the best interests of shareholders; if it is ignored, the consequence may well be vulnerability or poor performance. Good governance should facilitate efficient, effective and entrepreneurial management that can deliver shareholder value over the longer term."
>
> **Source: FRC, Combined Code, June 2008**

205 This view is underpinned by the preamble to the OECD's Principles of Corporate Governance, which sets out clearly the importance of Corporate Governance in the following statement:

> "The presence of an effective corporate governance system, within an individual company and across an economy as a whole, helps to provide a degree of confidence that is necessary for the proper functioning of a market economy. As a result, the cost of capital is lower and firms are encouraged to use resources more efficiently, thereby underpinning growth."
>
> **Source: OECD Principles of Corporate Governance, 2004**

206 At the same time as Corporate Governance promotes a positive system which is beneficial for the economy as a whole, there is also a strand which looks at the need for boards to have a role

in ensuring that there are effective "detective" controls (in other words, controls that help to identify shortcomings and failures) and overall monitoring of corporate activities. This view of Corporate Governance goes back at least as far as the Cadbury Report:

> "Had a Code such as ours been in existence in the past, we believe that a number of the recent examples of unexpected company failures and cases of fraud would have received attention earlier."
>
> **Source: The Committee on the Financial Aspects of Corporate Governance, known as The Cadbury Report, 1992**

207 Given the enormous collapse of market value during the current Financial Crisis, including in some cases the total elimination of banks as independent concerns, several aspects of these statements have clearly been breached:

- Company performance, by any standards, has been poor. Even the best performing banks have seen enormous reductions in their profitability and in their corporate value.
- Shareholder value, far from being delivered over the long term, has been destroyed on an enormous scale, and in many cases eliminated.
- The confidence that is needed "for the proper functioning of a market economy" has been substantially eroded in so far as inter-banking lending is still at very low levels, and trust is not being easily restored.
- The cost of capital has increased to the extent that the sole providers of capital for the restructuring of many banks have been either national governments or sovereign wealth funds.
- Far from receiving early attention, the failures, from Northern Rock, through Lehman Brothers to RBS appear to have been bolts from the blue.

208 In summary there are two conflicting philosophical arguments: the first, or what might be described as Corporate Governance-lite approach, is as follows:

> Corporate Governance is there to enable boards to discharge their duties as best they can in the light of prevailing conditions, but if the conditions are not favourable, then the board should not be held accountable because events were outside their control. In the case of the current Financial Crisis, the Perfect Storm has arisen and many financial institutions have succumbed as a consequence. No-one, within organisations or within the regulatory or political environment foresaw the problems, and as a consequence, no matter how good the Corporate Governance arrangements, no different outcome could have been expected.

209 The second, countervailing argument would run as follows:

> Boards have a responsibility to identify and understand the conditions within which their organisations are operating, to ensure that there is alignment between long and short term strategy, to ensure that remuneration policies are in line with the long term strategy, that ethical standards, risk management and assurance practices are appropriate so as to identify potential issues as soon as possible. Irrespective of the Perfect Storm, boards should have been trimming their sails to match the developing conditions and should have been cognisant of their responsibilities to a broader concept of society.

210 Under the first description of Corporate Governance, one would be examining whether different models of Corporate Governance would have made a difference. However, there are enough differences between the US and Europe to demonstrate that simple organisational issues would have made little difference. Under the second description, we would be examining whether there are improvements that can be made to Corporate Governance arrangements, which would help to prevent or at least alleviate the worst impacts of the Financial Crisis. If you adopt the first description of Corporate Governance, then the questions are purely about the board, its composition and its committees. If you adopt the second description, then the debate enlarges and becomes about how the tone and approach adopted at the board level are translated into the day-to-day activities of the organisation.

211 The balance of opinion from the interviews for this paper would suggest that we can and ought to take the more pro-active stance with regard to Corporate Governance.

212 RECOMMENDATION: As a matter of policy, boards should be encouraged to take a broad based view of Corporate Governance which encompasses the totality of their role. In addition those who maintain codes of Corporate Governance should ensure that a broad based view is incorporated into their respective codes. This may require changes in the law, which should be consistent across territories and it may also require considerable further work in developing appropriate guidance to assist boards and individual directors to discharge these duties.

III Corporate Governance Codes and Risk Management Guidance

301 There is an enormous array of source material when considering the strength or otherwise of any given code of Corporate Governance. Local laws, customs and cultures dictate approaches to Corporate Governance and colour the manner in which it is received by boards of directors, investors and other stakeholders. The review in this section is limited to three codes:

- The Corporate Governance Standards set out in the NYSE Listed Company Manual;
- The Combined Code produced by the Financial Reporting Council; and
- The Corporate Governance Code for listed Companies produced by the Associations Française des Entreprises Privées (AFEP) and the Mouvement des Entreprises de France (MEDEF).

All codes

302 Each of the three codes reviewed includes sections on the following topics:

- **Independent or non-executive directors:** all three codes envisage either a majority of non-executive directors or a balance of non-executive and executive directors. This is no longer a controversial issue. Each code either has material in it, or there is supporting material prepared by others that provides clarity on the meaning of independent.
- **Executive sessions:** all three of the codes envisage a need for non-executive directors to meet alone without the presence of executive directors, normally with access to such managers in the organisation as they require.
- **Nominations Committee:** all three codes require nomination committees for the appointment of new directors. The main purpose is to ensure that there is a transparent appointment process which is not under the control of management alone, and to ensure that the right balance of skills and experience is brought to the board table. In practice the search for new directors is often outsourced to headhunters with the consequence that the appearance of transparency is somewhat reduced by the typical reluctance of headhunters to consider shortlisting anyone who has not previously undertaken a given role. Consequently this can significantly reduce one of the objectives of the Higgs review in the UK which was specifically to encourage drawing potential board candidates from a broader population than hitherto.
- **Compensation Committee:** there is a requirement in each code for a compensation or remuneration committee. These are principally designed to deal with the remuneration of directors, and especially executive directors. In the case of the United States this includes the CEO and Executive Officers. Given the experience of the Financial Crisis, there is a good argument to be made that the scope of the remuneration committees should be increased to oversee the broad principles underpinning remuneration of senior managers throughout the organisation, especially where there is a high contingent of conditional remuneration (bonuses) which has the potential significantly to influence the nature of risk-taking in the organisation.
- **Audit Committee:** each code requires an audit committee of the board. There are similar requirements for the skills and expertise, although they have varying forces of law behind them.

- **Internal Audit:** all corporations are required to have internal audit under the NYSE code, are required to consider the need for internal audit on an annual basis under the Combined Code and Audit Committees are required to oversee internal audit under the French code.
- **Evaluation of board and committees:** all codes envisage the need for boards to conduct some form of evaluation of the boards and their committees. The Combined Code also requires an evaluation of individual board member performance.
- **Shareholder approval of equity compensation plans:** all of the codes require boards to approve equity compensation plans for director and, in the case of the NYSE code, for Executive Officers.

303 **RECOMMENDATION: Remuneration committees should oversee the broad principles underpinning remuneration of senior managers throughout the organisation, especially where there is a high contingent of conditional remuneration (bonuses) which has the potential significantly to influence the nature of risk-taking in the organisation.**

NYSE Code provisions

304 The NYSE Code has three unique components, being:

- **Code of Business Conduct and Ethics:** each company must develop and publish an appropriate Code of Business Conduct and Ethics. This is not explicitly required in either the Combined Code or the French Code. This absence may be explained by a presumption of high levels of business conduct and ethics. Revelations in the British and French press suggest that this presumption might be inappropriate. Accordingly, this type of provision should be incorporated in the codes where it is lacking.
- **Certification:** both the Combined Code and the French Code require companies to either comply or explain why they are not complying with their respective codes. The NYSE Code requires directors to certify that they are complying. Certification has an implication of a stronger requirement to comply with the provisions of Corporate Governance. Policy makers should consider whether boards in the UK and France have now had long enough to consider the benefits (to society at large) of good corporate governance and therefore that they should be required to certify compliance rather than simply explain why corporate governance is not relevant to them.
- **Public Reprimand Letter:** The NYSE Code is the only code that envisages the use of reprimand letters. Non compliance in the UK and France is essentially an area to be dealt with by investors. Policy makers should consider whether there is a role for naming and shaming companies that do not comply with the requirements of the Combined Code or French Code of Corporate Governance.

305 **RECOMMENDATION: As a matter of policy, mechanisms of enforcing compliance with Corporate Governance Codes should be reviewed. Such mechanisms need to be effective, easily implemented and should have teeth.**

European codes

306 European Codes of Corporate Governance have recently been subjected to European requirements. Several facets that are found in both the Combined Code and the French Code, but which are not in the NYSE code are:

- **Comply of explain:** as discussed above, the European codes require the boards to disclose the extent of their non-compliance with their respective codes and to explain why they have not complied. Evidence suggests that some of the disclosures under the Combined Code are mechanistic and remain unchanged from year to year. The purpose behind the concept of "Comply or Explain" is clear enough. However, the evidence of the Financial Crisis is that this in now an inadequate compliance regime, especially for companies which have a great societal impact, and policy makers should consider whether compliance should now be required unless compliance is not in the best interests of society, rather than the preferences of the directors themselves.
- **Separation of the role of Chairman and CEO:** Both the French and Combined Codes require the separation of the role of the Chairman and the CEO. This paper is recommending a re-balancing of the management and assurance roles of boards, and therefore it should be a requirement enshrined in all codes for the separation of the roles of Chairman and CEO, especially in companies where there is significant societal interest.
- **Availability of information:** both of the European Codes discuss the importance of information for the directors. Getting the balance right between inundating directors and starving them of information is of critical importance. Accordingly it should be the Chairman's role to ensure that this balance is struck correctly, and to facilitate any additional information that directors should request in the pursuance of their duties.
- **Periodic elections:** in Europe all directors are to be subject to periodic elections. This is not covered in the NYSE code.
- **Reporting to the market:** Both European Codes have provisions concerning the need to report to the market.
- **Use of AGM:** both the French Code and the Combined Code require companies to make good use of the AGM.

Combined Code

307 There are two particular provisions in the Combined Code which do not appear in the other two codes considered:

- **Role of institutional investors:** the Combined Code has a section on the role of institutional investors. Evidence suggests that the role of institutional investors in the proper discharge of corporate governance is immensely important. It may be that this would be more appropriately addressed in a code for institutional investors, rather than in the Combined Code which is more appropriately addressed to the board of directors. Policy makers should consider whether or not they should develop codes of practice or mandatory requirements for the involvement of institutional investors in the effective structuring and discharge of corporate governance in their investments.
- **Senior independent director:** the Combined Code includes a requirement for a senior independent director to be a separate channel of communication to the board. This role has

considerable merit and policy makers should consider whether such a role should be required in other codes.

French code

308 The French Code enshrines a provision requiring that directors represent all shareholders rather than specific segments interest groups. While it can be argued that this is the essence of "independent" directors, being explicit about the requirement is beneficial in the context of the current Financial Crisis.

309 **RECOMMENDATION: As a matter of policy, in order to reduce the scope for regulatory arbitrage, codes of Corporate Governance should be brought closer in line, as far as possible.**

Risk management

310 Risk management appears in each of the three codes to varying extents: in the NYSE code the requirement is for the Audit Committee to "Discuss policies with respect to risk assessment and risk management". This is explained further in the commentary as follows:

> "While it is the job of the CEO and senior management to assess and manage the listed company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the listed company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken. Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee."
>
> **Source: NYSE Listed Company Manual, Corporate Governance Standards, s303.A.07(D)**

311 The interesting aspects of this are that the expectation is that it is the job of the CEO and senior management "to assess and manage the listed company's exposure to risk". The Audit Committee's requirements are in respect of "financial risk exposures". There is no explicit requirement for the board to consider the risk management processes and framework as a whole.

312 The French Code deals with risk management in section 2.2 on off balance sheet items and corporate risks as follows:

> "Each listed company must be equipped with reliable procedures for the identification and assessment of its commitments and risks, and provide shareholders and investors with relevant information in this area.
>
> "For such purposes:
>
> - "The annual report should specify the internal procedures set up to identify and monitor off-balance-sheet-commitments, and to evaluate the corporation's material risks;

- "Each company must develop and clarify the information provided to shareholders and investors regarding off-balance-sheet-commitments and material risks, and disclose the company's ratings by financial rating agencies as well as any changes occurred during the financial year."

Source: Corporate Governance Code for Listed Companies, produced by AFEP and MEDEF, s 2.2

313 There is no further explicit guidance on risk management in the French Code.

314 The Combined Code deals with risk management in Part C on Accountability and Audit as follows:

> **The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets**
> **Code Provision**
> C.2.1 The board should, at least annually, conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational and compliance controls and risk management systems and risk management systems in relation to the financial reporting process.

Source: The Combined Code on Corporate Governance, published by the Financial Reporting Council, s C

315 This code provision makes an interesting, but somewhat impenetrable difference between internal control, risk management systems and risk management in relation to the financial reporting process. Further guidance is provided by the Turnbull Report as updated by the Flint Committee.

Sources of guidance

316 The two most commons sources of reference for further information are COSO and Turnbull. COSO, which is derived from the Committee of Sponsoring Organisations of the Treadway Commission, has produced two major works on risk management:

- Internal Control – Integrated Framework (1992); and
- Enterprise Risk Management – Integrated Framework (2004).

317 The first was a key part of the development of risk management, although it approached this from an internal control perspective. This was a major conceptual development which has underpinned a lot of current thinking on risk management. It described internal control as part of a process, rather than bolted on activities, and which had five main components:

- **A control environment:** without a good control environment there could be no effective internal control;
- **Risk identification:** this was the first time that control was seen as being truly a response to risk, which is an empowering concept because it also allowed people to identify wasteful control procedures;
- **Control activities:** these were the responses to risks, and they could either be preventive or detective controls;

- **Information and communication:** these were the glue that bound the whole internal control process together; and
- **Monitoring:** this was about making sure that the control activities, risk identification and control environment were understood at the top level of the organisation.

318 Each part of this model was designed to support three key corporate objectives:

- The continuity of the business;
- Timely and accurate financial reporting; and
- Compliance with local laws and regulations.

319 Finally, the third dimension of this model was that the control activities, in pursuit of these objectives was expected to be carried out throughout the organisation, whether at the head office, or manufacturing or distribution units throughout the organisation. The three dimensions of the COSO model are often shown graphically represented by a cube as shown in Figure 1:

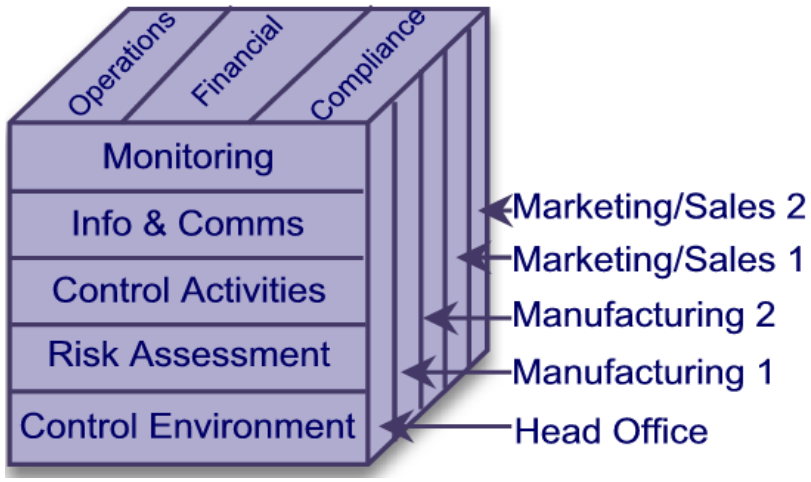

Figure 1: COSO Cube

320 The second COSO report, Enterprise Risk Management, developed the front face of the cube by adding three additional components:

- Objective setting;
- Event identification; and
- Risk response

321 It is questionable whether these additions add greatly to the model, since they were all inherently in the front face anyway.

Turnbull guidance

322 The updated Turnbull guidance provides a good conceptual overview of risk management. It re-iterates the board's role in managing risk and ensuring that there is a review of the effectiveness of internal control. Appendix 5 of the guidance provides some helpful guidance on the types of questions that the board should review in assessing the effectiveness of the risk and control procedures. The guidance is largely constructed around COSO style elements.

323 Neither COSO nor Turnbull provides effective guidance on how to implement their high level models into the reality of a complicated business. COSO retains a high level of following in the US, and Turnbull is widely recognised in the UK. Neither provides a helpful approach to the mechanics of creating an effective and lasting risk management and assurance framework over the long term.

Other Guidance

324 There are other sources of guidance in the public arena, including:

- AS/NZS4360 – The Australian and New Zealand risk management standard;
- BS31100 – the new British Standard on risk management; and
- The IRM/AIRMIC Risk Management Standard.

325 However, each of these struggles to provide comprehensive guidance which addresses all of the needs of major corporates in developing a risk management and assurance framework. Some common risk management problems are set out below.

- **Risks are frequently not linked to strategy:** Are risks linked to strategy? Is the strategy clearly articulated? Does the strategy set out how it will impact on the key value drivers? Aligning risks to the strategy is key to ensuring that risk management has a focus on the business context.
- **Risk definitions are often poorly expressed:** Are risk definitions capable of being interpreted by anyone (with appropriate local knowledge) who picks up the risk register? Better risk definitions (context, event, consequence) are contrary to a lot of current thinking in risk management which has been to abbreviate risk descriptions to the smallest number of words possible – that really does not work.
- **Can the organisation develop intelligent responses to risks:** Lots of risk registers dump everything into responding to risks. In fact there are five key dimensions to consider. ***Strategy****:* by which we mean do you want to prevent a risk from happening or allow it to happen and deal with the consequences, by, for example devising an appropriate contingency or disaster recovery plan. ***People****:* by which we mean do you want the risk to be managed by specific individuals, or is it something that needs to be managed throughout the organisation. ***Detail****:* by which we mean do you want to manage general risks or specific risks. ***Tasks****:* by which we mean the activities of gathering information, devising plans, procedures or approaches to managing the risk and then the actions, including implementing the plans, and looking for assurance that the proposed action has been taken. ***Drivers****:* by which we are referring to the need for someone or something to make sure that the whole process takes place. These drivers include managers in the organisation, outside regulators or the culture of the organisation.
- **Do boards take into account stakeholders and guardians in detailing responses to risk:** Does the risk management approach recognise the importance of people who are not directly involved in the management of a given risk, but who might be impacted if there is a change in the way it is addressed?
- **Is any more than lip service paid to the extended enterprise:** Are there important parts of the value chain that are outsourced to others, or where there is a dependence on key suppliers or joint venture partners? Do those outside parties manage risk as well as the principal, and in a manner which is compatible with their approach?

326 **RECOMMENDATION: There is a clear and urgent need for better guidance for directors on implementing and assessing risk management and assurance frameworks in large corporations. This guidance needs to be provided as an international framework that works across boundaries. It is probably not appropriate to use the International Standards Organisation (which currently has a draft standard: ISO 31000 on exposure) because of the nature of the compromises that are forced by the standard-setting process.**

327 It is interesting to note that the Core Principles for Effective Banking Supervision, as published by the Basel Committee on Banking Supervision, which set out the framework of minimum standards for sound supervisory practices, address the matter of risk management:

- Principle 7 – Risk management process: requires that banks have in place a comprehensive risk management process.
- Principles 8, 12, 14, 15 and 16 all address specific categories of risk.
- Principle 17 – Internal control and audit: requires that banks should have in place internal controls that are adequate for the size and complexity of their business.

328 **RECOMMENDATION: The international banking regulators should consider further how the Core Provisions for Effective Banking Supervision which relate to the matters of Corporate Governance as set out in this paper are dealt with effectively both by the national supervisors, and also by the banks themselves.**

IV A distressed model of Corporate Governance

401 It would be unfair to say that the Financial Crisis was exclusively caused by poor Corporate Governance: many other factors played their part, including variable quality regulatory oversight, questionable political oversight of the system and fundamental economic conditions. While it is not currently possible to prove this without considerable additional research, the general expectation is that those institutions that have weathered the storm best are those with the best embedded Corporate Governance models and those that have fared worst were those with poor Corporate Governance models. Furthermore, it is arguable that even if Corporate Governance is not a cause of the Financial Crisis, it has to have been at least a contributory factor in its severity.

402 Based on the interviews conducted for this paper, the consensus of opinion is that the models of Corporate Governance employed in the US, the UK and France are at least distressed, if not broken. The reasons for making this assertion are set out in the following paragraphs.

A high level view of Corporate Governance

403 Perceptions of Corporate Governance vary. Some interviewees regard Corporate Governance as being something that resides only at the very top of an organisation: the number of non-executive directors, the composition of the Audit and other committees and so on. These individuals would also recognise the importance of risk oversight and setting the tone from the top. Others would see Corporate Governance reaching down into the organisation, with a much more direct relationship with internal audit, the ethical behaviours of the staff and having a deep and meaningful relationship with the organisation.

404 It seems strange that the formulae of modern Corporate Governance have developed an almost unhealthy view of risk oversight as focussing exclusively on the internal and external auditors. While the Smith Report in the UK (as adopted into the Combined Code) and the NYSE Listing Rules talk about risk management, as described in Section 3 of this report, there is little guidance as to how, apart from by reference to auditors, they can discharge these risk responsibilities. Where there is guidance (for example COSO or the Turnbull Report) the guidance is so high level that it is hard to identify any particular benefit from the guidance.

Compliance is (almost) voluntary

405 Compliance with current Corporate Governance frameworks is not onerous compared to other more legalistic director responsibilities. For example, failure to comply with certain provisions of the Sarbanes-Oxley Act could lead to significant financial penalties and lengthy custodial sentences for directors. Even under the Companies Act in the UK, there are penalties for failing to comply with some provisions which could result in criminal convictions – and these can be comparatively minor items such as a failure to file the annual accounts on time. Equally, failure to observe other regulations could result in significant penalties to the company (for example Anti-Trust provisions in the US and in Europe), or the revocation of licenses to operate, either for the organisation or for particular individuals (for example the Financial Services Markets Act in the UK). However, there are no legal requirements to comply with Corporate Governance codes. This contradiction is hard to reconcile philosophically with the raft of penalties and legal liabilities that directors face in many other areas of regulated life: to put this in context Sarbanes-Oxley envisages

up to forty years imprisonment for failing to comply with its regulations, and yet directors face no personal criminal liability when global banking institutions fail.

406 In the absence of legal requirements in Europe there are three principal drivers in the banking sector towards compliance with the codes of Corporate Governance:

- Voluntary self-regulation;
- Investor pressures; and
- Regulatory oversight.

407 In addition in the US there is a regime of "Reprimand Letters" from the NYSE, and the ultimate sanction of suspension or de-listing.

Voluntary self-regulation

408 The UK and, more recently, the French codes of Corporate Governance are based on the need to "comply or explain". As the Combined Code indicates, there is an expectation that there may be valid reasons for non-compliance and moreover "the flexibility it offers is valued by company boards and by investors in pursuing better corporate governance." In practice there are some companies that have failed to comply or to provide adequate explanation for several years in a row. None of these breaches is subject to any further ramifications unless investors decide to take the matter further.

409 Some interviewees question the efficacy of a "comply or explain" regime in that it demands:

- A high degree of sophistication on the part of the board to identify the long term benefits that should accrue to the organisation by properly complying (or explaining non compliance); and
- Pressure is assumed from an equally sophisticated and discerning investor community, which might not be in evidence.

Given that these are organisations that have a high societal impact, it may be that this approach of "comply or explain" is no longer sufficient.

Investor pressures

410 While the Combined Code encourages a discourse around non-compliance, in practice the policing of the code becomes a matter for large investors and their relevant associations. There have been some celebrated challenges to non-compliance, but they are relatively few and far between. It might be argues that this merely reflects good corporate behaviour and the requirement in Paragraph 5 of the Combined Code as follows:

> "If a company chooses not to comply with one or more provisions of the Code, it must give shareholders a careful and clear explanation which shareholders should evaluate on its merits. In providing an explanation, the company should aim to illustrate how its actual practices are consistent with the principle to which the particular provision relates and contribute to good governance."
>
> **Source: FRC, Combined Code, June 2008**

Regulatory oversight

411 It is clear that there are different approaches adopted each side of the Atlantic to regulatory oversight of Corporate Governance in banking institutions. The FSA has long taken an active interest in individual board members, their skills and background and suitability for the role as a board director. This is in the course of being enhanced also to include the board membership of bank holding companies. On the other hand, the SEC tends to take a more hands-off approach. It rarely interviews individual directors, preferring to concentrate on compliance with the strict letter of the appropriate regulations. For example, one individual who is both on the board of a major US organisation and also a smaller British organisation has regularly submitted papers demonstrating his independence to the SEC and has yet to meet with anyone from the SEC. In contrast he has met members of the FSA's regulatory team to discuss how he and other board members discharge their responsibilities in the UK.

412 The days of a "nod" or "shake of the head" from institutions such as the Bank of England are long gone. However, given the turmoil that we have seen, it is clear that regulators are going to have to demonstrate a more active and explicit role in board membership, and in the discharge of Corporate Governance duties by the boards of banks as a whole.

NYSE compliance regime

413 The NYSE code requires annual certification to the Stock Exchange of compliance with the code and furthermore "Each listed company CEO must promptly notify the NYSE in writing after any executive officer of the listed company becomes aware of any material non-compliance with any applicable provisions of this Section [on Corporate Governance]." The NYSE also envisages a regime of "reprimand letters" for non-compliance:

> **"The NYSE may issue a public reprimand letter to any listed company that violates a NYSE listing standard.**
>
> "*Commentary:* Suspending trading in or delisting a listed company can be harmful to the very shareholders that the NYSE listing standards seek to protect; the NYSE must therefore use these measures sparingly and judiciously. For this reason it is appropriate for the NYSE to have the ability to apply a lesser sanction to deter companies from violating its corporate governance (or other) listing standards. Accordingly, the NYSE may issue a public reprimand letter to any listed company, regardless of type of security listed or country of incorporation, that it determines has violated a NYSE listing standard. For companies that repeatedly or flagrantly violate NYSE listing standards, suspension and delisting remain the ultimate penalties."
>
> **Source: NYSE Listed Company Manual, s303A.00 Corporate Governance Standards, November 2004**

Investor pressures

414 For many years, bank boards have been almost without exception subjected to intense pressure from institutional investors to improve performance, increase efficiency, reduce capital, engage in markets for ever more complicated instruments and to reduce their capital to the extent possible. Where bank boards resist, they find themselves subject to adverse comment and aggressive shareholders seeking to "unlock" underperforming organisations. As a consequence, cautious board members were likely to find themselves removed as more compliant directors were

installed, or removed as their organisations were acquired. Of course, it is fair to say that the investors themselves were also being pushed to demonstrate increasing performance in their funds.

415 Combined with this relentless pressure, it is clear that a "herd" mentality develops amongst the investors and bankers alike. This encourages a headlong and at times, inappropriate rush into products that are untested and in some cases poorly understood. It takes a brave individual to declare in a product review meeting that they do not understand the new instrument, or for a commentator to expose "the Emperor's new clothes", woven as they are from the finest minds in the industry. As Chuck Prince, former CEO of Citigroup, said: *"When the music stops, in terms of liquidity, things will be complicated. But as long as the music is playing, you've got to get up and dance. We're still dancing."*

Source: Chuck Prince, Financial Times, July 10 2007.

416 Without a doubt, investor pressures have forced management to seek ever greater performance from their businesses. This growth soon becomes a cultural expectation in organisations with managers' behaviours anchored at increasingly higher levels of performance. This is then reinforced by aggressive remuneration policies that reward compliant behaviour. There is something of an inevitability that this behaviour will create an inherently unstable environment.

417 This might best be described as capitalism in its fullest glory. A sight that is hard to challenge in the height of a long and sustained bull market. According to at least one commentator, the fact that investors are now bemoaning lost capital, devastated share values and destroyed markets has an edge of hypocrisy. But what is absolutely clear is that it is not possible for banks sustainably to maintain high credit ratings and pursue top-quartile returns throughout the cycle. Inevitably as the cycle begins to turn down, one of those twin objectives will have to be sacrificed.

Non-executive oversight stretched

418 One might argue that it is part of the role of non-executive directors to exercise a degree of caution in the boardroom that enables the executive management to consider with more clarity the consequences of running with (or even ahead of) the market. One audit committee member of a large US banking institution commented that it was the board's intervention that had prevented this particular organisation from a potentially disastrous acquisition in the mortgage market. The sense of the board was that the market was at or near the top and that the economy was at a tipping point. As a consequence the board withdrew the proposal and subsequently came back with a much more modest acquisition strategy that proceeded. Clearly therefore, good boards can act as a restraint on the growth aspirations of the executive when those aspirations conflict with the overall health of the organisation.

419 In contrast however, as noted in the hearings of the Treasury Select Committee in the UK, not a single non-executive director sought to block the acquisition of ABN Amro by RBS, an acquisition which even while it was being pursued, was regarded by many commentators as being overly aggressive and executed at the top of the market. The former Chairman (Sir Tom McKillop) has commented in his evidence to the Committee that the entire value of the goodwill in the acquisition has had to be written off.

420 On the other hand it is fair to say that the very significant majority of directors have the interests of their organisations at heart and seek to discharge their duties, including those in respect of oversight, to the best of their abilities. With this in mind, all boards are expected to:

- Have meetings of non-executive members of boards without executive managers present;
- Meet (in the form of Audit Committees) with both internal and external auditors without the presence of the management; and
- Have arrangements for whistle-blowing reports to come to the non-executive directors.

421 And yet a common theme from the interviews was that the amount of time available to non-executive directors to discharge their duties is necessarily limited. In effect much of this risk or assurance oversight falls to the Audit Committee members. Few non-executive directors have more than an absolute maximum of 20% of their year to devote to any given board, and in many cases their attendance at meetings may be as little as fifteen days a year.

422 In discharging their duties, boards in the US model, and non-executive directors in the UK and French models of Corporate Governance can only be as good as the information that is provided to them, or to which they have access. So while they may be able to meet key individuals (Head of Internal Audit or the External Audit Partner) as of right, and others by arrangement with management, the length and depth of board packs is inevitably variable. Some complain of too much information (what might be described as the Ford syndrome, where the answer to any question that had ever been asked by a director was supplied for ever more – this may be an urban myth, but it makes the point) and others complain of too little information and insufficient time to delve any deeper.

Public accounting and external audit stretched to breaking point

423 One of the fundamental tenets of current corporate governance around the world is the importance of the external or financial audit. Conducted by an independent organisation, the theory is that the auditors opine on the accounts to confirm whether or not they reflect an accurate portrait of the organisation for the previous year and at the balance sheet date. At the time of the origin of the audit this was seen as being a sufficient process to report to owners who were by then separated from the management. Audit would have addressed many of the perceived key risks at the time, and which were largely seen as being financial in nature. The model has struggled over the course of the twentieth century to keep up to date with stakeholder perceptions. For example, audit is not expected to identify all frauds, and yet there is still a perception in some comparatively sophisticated quarters that it should do so. In the UK, the audit profession spent a considerable portion of the eighties addressing the perception gap. However, it would seem that the gap between what the users of the accounts (politicians, the public, the economic system) believe they can read into the accounts, and what the auditors mean when they opine, continues to grow. A “clean” or unqualified audit report is seen as a general badge of health for the organisation, and yet in reality the audit is addressing a diminishing proportion of the risks that an organisation faces.

424 This is exacerbated by the comparative rarity of issuing a qualified audit report, which in itself has the potential to be the final demonstration of frailty that could bring a bank down. It might make sense for the audit profession, in conjunction with the banking industry and regulators, to explore whether a much more gradated approach to audit reports could be developed which would

be less binary in its application, but which could signal more subtle differences between banks without catastrophically undermining the bank in question.

425 For the most part the accounts are little more than a series of rearward looking financial key performance indicators that have been drawn up on the basis of normative accounting rules which may well render the data increasingly inappropriate for decision making purposes. Of course the accounts are normally drawn up under the "going concern" principle, which pre-supposes that the organisation will continue to exist throughout the following reporting period. But neither the financial statements, nor the audit address many of the forward looking risk issues that are of interest to stakeholders today. In particular they do not address the sustainability of the business model, nor do they look in any depth at systemic risks in an industry or economy as a whole, even though in the current era of significant concentration of the audit market (no major bank is audited by a non Big-4 Firm of auditors) it ought to be feasible to benefit from their collective knowledge across the sector.

426 In an era where inter-connectivity and inter-dependence is of a different order of magnitude compared to the origins of the audit process, it is not surprising that the audit model has been shown incapable of addressing the concerns of the modern economy. This inability to deal with the modern spectrum of risks that interest the stakeholder can only be exacerbated in a litigious environment where joint and several liability is destined to hold back any innovation in the audit process which will inevitably expose the livelihoods of the auditors to the capricious whim of the legal system.

Internal audit struggling

427 Over the last two decades, internal audit has undergone a transformation in its role, remit and attitudes. In many organisations internal audit has moved from being an extension of financial control, focussing on financial accounts and the operation of routine internal financial controls to becoming a function which perceives it has a role in assurance and internal consultancy, in relation to all risks, but especially those that have an impact at a strategic level, and which has a reporting line directly to the chair of the Audit Committee. In practice however, the identification of risks is weak in many organisations and the role of internal audit in running risk identification processes is hotly debated. Internal auditors frequently lament that they are not asked more questions by Audit Committees and feel that they are not used to their full potential.

428 The ambition of internal auditors is both to provide assurance and to be a catalyst for improvement. In practice, given the relative numbers of internal auditors to staff, it is unreasonable to expect them to operate and apply controls (which is what some people still think of them doing). Therefore the only practical way for internal audit to add value is to look at the whole – how does the system of internal control operate to manage the risks to the objectives of the organisation? It is also worth noting that internal audit does not usually view itself as an extra level of risk management – there are not enough internal auditors to identify risks, but they do have a role to champion the management of risk, to challenge and get to the truth and to catalyse the change. The catalyst point is important because, internal audit departments don't have the staff numbers to change things on their own. They have to work inside the organisation, getting the staff, managers and boards to authorise, resource and implement change. In the environment that has been

discussed elsewhere in this document, that has been an uphill struggle. In a sense this represents a diversion from the essential assurance role.

429 Over the last ten years there has been a significant move for internal audit to report to Audit Committee chairmen. This shows the beginning of an evolution that might help to tackle some of the problems referred to in this report. This provides the Audit Committee with a knowledgeable source of information from someone who has an assurance focus.

430 Non executive directors and Audit Committee chairmen are often surveyed and respond that:

- Heads of internal audit are not up to the job;
- Internal audit lacks adequate independence;
- They rely more on external audit;
- They have not properly defined the role that they wish internal audit to fulfil.

Whether one can extrapolate from broad surveys across all industries into the specifics of the banking industry is not clear. However, the risk remains that internal audit in many institutions may be no more highly regarded by the board than is the norm across the business world.

Where does assurance come from?

431 This therefore begs the question as to where assurance can possibly be drawn from. If:

- Audit Committee members are overstretched;
- The relevance of external audit is being over emphasised; and
- Internal audit is not all that it might be;

432 Then where can board members draw comfort in respect of their responsibilities for assurance. They can of course:

- Seek the views of the regulators. Although it is worth noting that in the view of at least one interviewee, the degree of personal intervention (ie talking to board members) is much higher in the UK than in the US, where the interaction is much more process-oriented (eg: do you meet the requirements for independence? Rather than: how do you go about the job?)
- Seek the views of financial analysts. Except of course, in many cases the financial analysts are part of the pressure imposed by the investor community.
- Seek the views of the rating agencies. However, the views of the rating agencies may well be coloured by the commercial pressures that they have faced in assessing credit ratings for the increasing number of investment vehicles.

433 Internally, board members can seek assurance from other members of the management team, including the Risk Management department. Although in a sense the current organisation of risk management has been about the nuts and bolts of risk and spreadsheets, rather than a coherent assessment of the full range of risks that the organisation faces. Therefore if the risk management group is not looking at a particular type of risk, there will not be any focus on it for the purposes of the board seeking assurance.

434 The board can also seek additional assistance from the General Counsel or Company Secretary, or from other managers in the organisation. But this all takes much more time that the already heavy workload of the average non-executive director would allow.

435 **RECOMMENDATION: As a matter of policy, there should be a new focus on the assurance role of the board, and how that should be discharged. Often referred to as oversight, this implies a rather passive role. By introducing the term "assurance", boards should be encouraged to be more pro-active in this role.**

V A new duty of care

501 It is not the purpose of this paper to generate a lawyers' charter or to create a new bureaucracy. However, having identified that Corporate Governance has struggled, and indeed failed, to cope with the Financial Crisis, it is incumbent on us to explore how we might address the shortcomings. One of the major issues is the need to persuade boards and individual directors that they need to take their Corporate Governance role seriously, and to provide the investment in time which it requires. In many cases this is anathema to boards where directors often seen themselves as providing strategic oversight and contributing personal expertise gained in other roles.

502 Corporate Governance is not a question of ticking the boxes of relevant codes, but rather it is as much about the board's role in providing risk oversight as it is about supporting management in implementing its strategy. Most non-executive directors dislike the increasing role of Corporate Policeman that seems to be foisted upon them. However, it is clear that some part of the board's responsibility is to act as a counter-weight to the often risk-laden growth aspirations of some management teams.

503 Many interviewees have referred to CEO's as dominant, persuasive individuals who are used to getting their own way within their organisations. Some have been described as "imperial", others have been described as "bullying". The exact terminology is unimportant; the implications of their behaviours are the important focus. However, there is no question but that investor pressures on these individuals to perform and to grow their organisations are very great. Failure to grow in line with market aspirations and expectations can and will cut short the tenure of the incumbents. This focuses the mind and necessarily the demands that the CEO's in turn place on their entire organisations. Spurred on by an engrained culture of aggressive growth and encouraged by the promise of exorbitant bonuses, departmental managers prepare budgets and plans that their people are expected to achieve almost by whatever means possible. Unsatisfactory budgets and plans from business units are rejected and failure to meet targets is punished by reduced remuneration of even the loss of jobs. This tends to lead to an excessively short-term approach, rather than to long term, sustainable value creation.

504 One can make the argument persuasively that this is the life-blood of market capitalism. However, what this approach fails to do is to protect the interests of those who have no financial impact on the short term results, but who can be disproportionately prejudiced by the decisions of the short-term oriented CEO or corporation. In the case of banks, society at large has deemed that depositors are such a category and that they deserve special protection. During this Financial Crisis, in the vast majority of cases around the world, deposit-taking institutions have been afforded a level of protection vastly in excess of national deposit protection schemes. In effect some Banks have been deemed "too big to fail" and either have been shepherded into mergers, have been acquired by the state, or have had the totality of their deposits guaranteed. The banking institutions that have been allowed to fail have not on the whole had direct dealings with the public, although the knock-on effects have been catastrophic to trust in the banking system.

505 This level of protection makes the banks (and some insurance corporations) different to most other organisations (with perhaps the exception of the car industry in the US and the UK).

506 **RECOMMENDATION: In the case of organisations that have a broad societal impact, and who therefore owe a duty of care to society at large, directors and officers should owe a legal duty to discharge their Corporate Governance responsibilities with due and diligent care. This legal duty should be broadly equivalent in all jurisdictions to avoid regulatory arbitrage.**

507 The relevant banking supervisors or regulators should conduct a periodic assessment of the manner in which directors and officers discharge this duty, both as individuals and as a board. While details would need to be worked out, the duty would address:

- The normal areas of Corporate Governance as already set out in the relevant codes (see Section 3 for a comparison of existing codes). However, it might be worth exploring whether there is scope for greater harmonisation of the codes.
- An enhanced role addressing risk oversight and assurance (see the next two sections of this paper for more details).

508 What are not discussed in this paper are the exact mechanisms or responsibilities that would be owed under this duty. This would need to be addressed at an international level. In addition there would need to be some form of "Safe Harbour" provision for those who have undertaken their individual responsibilities with due and diligent care, but who nevertheless find their organisation to be failing.

509 **RECOMMENDATION: The code developers and the international banking regulators should review the Codes of Corporate Governance that societally important banks are required to comply with, that these codes should where possible be harmonised with the requirements of the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision and should take into account the recommendations made elsewhere in this paper.**

Professionalization of the board

510 In support of this initiative, it might be appropriate to consider the "professionalization" of boards and the "C-suite". The UK Treasury Select Committee suggested in response to the collapse of Northern Rock that board directors should have a "banking" qualification. It seems highly unlikely that a first or second degree, or a professional qualification taken immediately after graduation, would have a great deal of impact on a role taken on some thirty or more years later. However, there is an argument to suggest that an individual's "license to operate" should be subject to review in the event of inappropriate behaviours.

511 This would imply a licensing regime, perhaps akin to that effectively operated by professional bodies such as the ICAEW or the ABA, which would be earned either by experience or by examination, and subsequently maintained by Continuing Professional Development. One might argue that in the current environment that this would be entirely irrelevant since none of the key board members of failed institutions is likely to be employed again in a similar role. However, there is some evidence to suggest that members of professional bodies such as those referred to, have a sense of professional duty that is owed to society at large, and outside of their current employers, based upon the retention of their license to operate. Examples such as the Institute of Directors' professional qualification may prove to be a fertile ground for further development.

512 **RECOMMENDATION: The international banking regulators should initiate a programme for the professionalization of management in the banking sector. This would involve the ultimate introduction of a professional qualification. This should be overseen by a new professional body which would award the qualification, oversee professional ethics and act as a guardian of high standards of professional behaviour by individuals. Members of existing professions might remain subject to their own professional codes, although there might need to be a meta-professional code that cuts across all professions in the banking sector.**

VI A risk framework

601 One of the most startling aspects of this Financial Crisis is that virtually nobody saw it in the making, and those that did were ignored. Investors were pushing for growth right up until the last minute. Bankers were, in Chuck Prince's words, dancing. Regulators and Central Banks did not put the brakes on banking activities, and politicians were, on the whole, continuing to work closely with the grain of the financial services markets.

602 Unethical and possibly illegal loans were being marketed in the United States, 125% mortgages were being made available in the UK, and credit was being fuelled by "cheap" liquidity. New financial instruments which were meant to spread the risk were being created and then rated by the rating agencies. Institutional investors were demanding ever greater leverage, more efficient use of capital and better returns. Work by the FSA in the background to nudge organisations like HBOS and Northern Rock to better operating and risk models appears to have had little effect.

603 This despite the fact that all of the banks had senior risk managers and supposedly comprehensive risk programmes. Many were moving towards or had achieved AMA status for Operational Risk under Basel II. Many of the larger banks had very sophisticated credit and market risk programmes and conducted extreme stress testing as periodically required by their banking regulators. The banks considered themselves to be risk experts: where car companies had a core competence in designing, manufacturing and marketing cars, banks had a core competence in identifying, leveraging, transforming and spreading risk: hence their perceived status as masters of their risk universe.

604 Despite their risk programmes boards did not foresee the Financial Crisis. In part this might have been because of a failure by individual directors to understand the nature of the risks that their banks were assuming. This point was reinforced by the evidence of former Chairmen and Chief Executives to the Treasury Select Committee which is looking into the lessons to be learned from the Financial Crisis:

> **Chairman:** "Can I ask each of you, did you personally understand the full complexity of these vehicles that your clever young men were creating?"
>
> **Sir Tom McKillop:** "You said 'full complexity' and I would say no."
>
> **Source: Treasury Select Committee of the House of Commons. Taken from an uncorrected transcript of evidence taken in public and reported to the House. Neither witnesses nor Members have had the opportunity to correct the record. The transcript is not yet an approved formal record of the proceedings.**

Earlier in the discussion, Sir Tom also said of the nature of the risks that RBS was assuming: "We had no idea of the speed and the interconnectedness and how quickly it could all have turned out."

605 The picture that emerges is one of comparative bewilderment at the nature and scope of the risks. Where they were identified, as for example in the case of HBOS's dependence on wholesale market funding, corrective action was only initiated too late for it to have a significant corrective benefit to the risk impact.

606 In the course of interviews for this paper, it has become apparent that there is a disconnect between different aspects of risk. On the one hand, what John McFall (Chairman of the Treasury Select Committee) refers to as "clever young men", were creating new instruments for disseminating risk, others were exploring credit and market risk and yet others were looking at operational risk. And yet, in discussion with a senior risk manager at one of the large banks, it became apparent that their "enterprise risk management" approach was still at a very early stage. This implies that there was not yet a joined up approach to risk management across the bank.

607 Based on the interviews for this exercise, it is clear that:

- Bank risk processes are very focussed on operational (as opposed to strategic) risks;
- There is comparatively little emphasis on developing a risk aware culture; and
- The remuneration culture has skewed risk taking towards potentially dangerous risk profiles.

608 As a senior member of the FSA said, it is not difficult to envisage a bank that has twin objectives of AA+ credit rating and 25% per annum growth finding those objectives soon come into conflict. It is not clear that many banking organisations would have explicitly considered the conflicting nature of their major objectives and accordingly they would not have been able to express their risk appetite, let alone tie the operational risks that emerge from their risk models into their strategic impact.

609 **RECOMMENDATION: Where their complexity demands it, banks should be encouraged to develop more sophisticated holistic risk frameworks within which they can manage risk better.**

610 It is worth noting that prior to its demise, Rick Buy, the risk manager at Enron Corporation was seeking, in his own words:

> "...to condense all the risks of Enron Corporation into a single metric. This would comprise operational, market and credit risk and incorporate risk-adjusted return on capital (RAROC), value-at-risk (VaR) and extreme value theory into what Buy calls a single 'pseudo capital-at-risk figure' that can be shown to the Enron board of directors."
>
> **Source: E-Risk, February 2001**

It is not proposed that any banking institution should seek to reduce its risk reporting to a single figure: that clearly is not feasible or desirable. However, there needs to be a recognition that risk taking needs to be balanced with avoiding value destroying events (pitfalls) and equally takes into account the conflicting pressures from the performance culture (and more particularly in the banking sector, short term cash bonuses that are not aligned to the long term strategic objectives or the risk profile of the bank) and the corporate ethics and behaviours which their societal impact demands from the banking sector.

611 **RECOMMENDATION: Banks should be encouraged to think in terms of a balanced risk approach which balances the behaviours associated with the risks being taken and those being avoided, and which is also cognisant of the risks associated with its performance culture and ethical approach to business.**

612 This recommendation will require a significant change of culture in order to embed a "risk intelligent" approach to business within these organisations. Some areas where further consideration should be given to encouraging banking institutions to developing aspects of their risk management are set out in the paragraphs below. Appendix B sets out some further thoughts about a possible approach to Balanced Risk.

Risk intelligent organisations

613 Many organisations, including banks, see the corporate governance aspects of risk management as a paper pushing exercise that adds little value. It is clear that risk management needs to move beyond the mundane processes and needs to become part of the culture of organisations. In other words risk management needs to be about bringing a perspective to the management of complicated issues in complex organisations. It should be about the management (and not the avoidance) of risk. It should help to prioritise work in a fast moving context with an approach that is better than simple intuition and which facilitates communication between people. Risk management needs to become a style of thought, and should definitely not be a mere paper chase. Developing a risk intelligent organisation requires boards to understand the maturity of their risk management activities right across the organisation.

614 **RECOMMENDATION: All banking institutions should periodically assess their risk management maturity and identify what steps they need to take in order to develop into Risk Intelligent Organisations.**

615 The Institute of Internal Auditors in the UK and Ireland (the "IIA UK") encourages organisations to look at their risk management maturity. IIA UK focuses predominantly on risk processes. In addition, boards should consider four aspects that need to be assessed on a regular basis:

- **Manager and staff attitudes to risk, control and governance:** based on the experience of working with a multitude of different clients in different sectors, attitudes to risk, control and governance are perceived differently in different parts of any organisation. It is clear that it is important that the board has an overall understanding of these attitudes so that it can assess what further steps are required to develop the overall culture of risk management.
- **Whether the organisation is prone to disasters:** there is plenty of material in the risk management literature to identify signs of the disaster-prone companies. Banks might well have been able to hold a mirror up to themselves and identify many of the symptoms of such companies (for example excessive complexity, blame cultures, over-confidence, following the herd and so on). Boards need to undertake this exercise round all parts of the business to identify whether any remedial action needs to be taken.
- **Attitudes to corporate ethics and behaviours:** many organisations pay little more than lip-service to corporate ethics. Surveys have shown that a high proportion of staff have seen potentially illegal or inappropriate behaviours in others that they in turn are not prepared to report in the company. Facilitating appropriate corporate ethics with a focus on open and frank disclosure is important to a balanced approach to risk management.
- **Identify how staff will react in times of pressure:** many risk management systems assume a normal pace of life for the business. These systems then crash when excessive pressure is

applied because managers and staff move into a different paradigm of management, which results in the need for what might be described as Fast Clockspeed Risk Management. Part of this assessment is also about understanding the heuristics that managers and staff use to manage risk. Most informal risk management is done by means of the "unwritten rules of the game" – identifying and understanding the ramifications of those unwritten rules are both vital.

616 **RECOMMENDATION: Boards should take formal responsibility for setting, managing and periodically assessing the risk management culture of the organisation. This will facilitate a better approach to managing risk throughout the organisation.**

Scope of risk management

617 At the moment, risk and risk management mean different things to different people. In the course of one day of its deliberations the Treasury Select Committee identified risk in:

- Acquisitions (RBS's acquisition of ABN Amro);
- Financial instruments;
- The sales culture (the FSA's comments on HBOS sales culture, as reflected also by the former Head of Group Regulatory Risk at HBOS); and
- Dependency on wholesale funding.

618 In addition the well documented problems of unauthorised trading at Société Générale represent a further manifestation of risk, as do the sub-prime lending problems in the US and the total destruction of trust following the collapse of Lehman Brothers which led to the drying up of inter-bank lending.

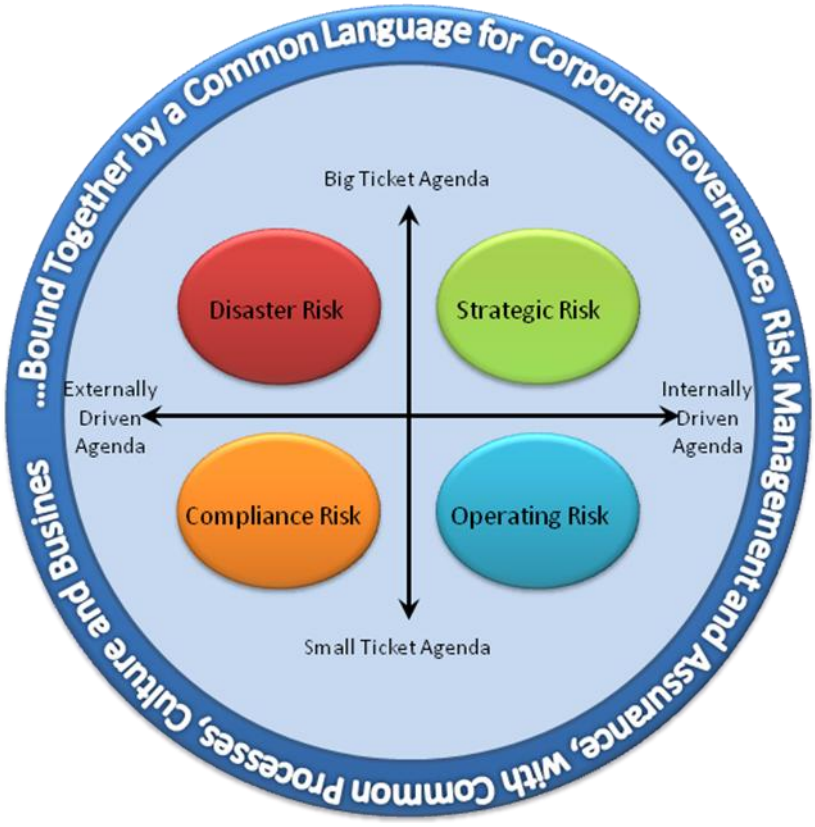

Figure 2 - Scope of Risk Management

619 This diversity of risk leads to considerable difficulties in bringing all of the risk elements together, and all organisations, not just banks, tends to obsess about some elements of risk management and to omit others from its group thinking about risk. Figure 2 sets out one possible way of thinking about the scope of risk management and ensuring that all aspects are considered. Turnbull concentrated on the top right hand quadrant, without

understanding the component parts, and Sarbanes-Oxley on the bottom left hand quadrant, without looking at the bigger picture. Nightmare risks are often those that move rapidly from the bottom of the scale to the top and become big ticket issues – for example funding operations from the wholesale market at HBOS probably started as an operating risk, but developed into a major strategic issue which ultimately brought the bank to its knees. Many organisations fail to see these changing risks coming at them because they are culturally attuned to an on-going level of activity that provides false comfort. A good risk management framework will address all of these areas.

620 **RECOMMENDATION: Boards should take formal responsibility for setting the scope of risk management activities right round the operations of the institution and its business activities to ensure that risks are identified, assessed, managed and monitored in an appropriate manner, in the light of the risk culture.**

The single voice of risk management

621 As indicated above and in Figure 2, it is not uncommon for risk management to mean different things in different parts of an organisation. Typically there is a different meaning of risk management for each of governance, risk departments and internal audit. This can lead to considerable confusion, to people failing to understand differing responsibilities, believing that they are being discharged elsewhere and to important risk issues falling between organisational gaps and between risk silos.

622 **RECOMMENDATION: There should be a single meaning of risk management in each institution which encompasses different roles and responsibilities, and which facilitates information and communication between different parts and different levels of the hierarchy within the organisation. The definition should be agreed and communicated by the board.**

Granularity of risk management

623 Financial and management reporting have been focussed for centuries on currency based reporting. From the 14th Century innovation of double entry bookkeeping by an Italian monk, money has been the cornerstone of reporting and decision making. In the latter half of the 20th Century and up to the current time, more difficult and subjective areas of accounting (such as valuation of investments in a trading book, deferred taxation, revenue recognition) where there is scope for manipulation of the results or balance sheet values have been subjected to normative accounting rules.

624 The benefit of accounting in monetary terms is clear: the unit of currency is recognised, and most transactions are reflected in monetary terms. Organisations capture accounting data at a very low level of granularity. At one of the author's former clients, the group financial controller used to allocate his lunch across five different cost centres so that all bore their fair share of the costs associated with his travel and subsistence expenses. This is clearly excessive, however, it illustrates the point that as a consequence of the level of granularity and based upon the rules, it is possible for any company to state unequivocally its revenues, or its profit after taxation, or the amortised value of its fixed assets. The relative sizes are clear, that they are made up of lots of sub-accounts is well understood and the systems for recording transactions are commonplace.

625 This is not the case with risk management. When John McFall or Sir Tom McKillop talk about the risk associated with the acquisition of ABN Amro by RBS, they are in fact talking about a multitude of different risks, which might include exposure to toxic assets, variable quality credit risk processes, unknown operational risk procedures, the culture of risk taking and so on. The exact taxonomy of risks involved in such an acquisition would differ for each transaction and depending on who was undertaking the acquisition: for example, had a risk due diligence exercise been carried out by Barclays when they first mooted a takeover of ABN Amro, it would no doubt have looked very different to a similar task undertaken for RBS and its acquisition partners. To a large extent the differences would be valid: they would relate to different new holding companies, and to different corporate objectives. However, some of the differences would simply be because two different sets of individuals were carrying out the analysis.

626 At the moment there is no single recognised way for organisations to link high level aggregate risks to low level transactional risks. As a consequence, those who are analysing risks, for example of individual CDO instruments, might not have been able to attach them effectively to the high level of aggregation which is necessarily involved in board discussions. While some risk experts talk about a "golden thread" linking from the top to the bottom, others seek a more rigid alignment between objectives, risks and controls (sometimes referred to as ORCA – objective, risk and control alignment). In any event it is unequivocally the case that there is no single direct line from top to bottom: there are one-to-many, many-to-one and many-to-many relationships between risks and between risks and controls.

627 While IT systems have been developed to address many of these issues, there are more important definitional issues to be ironed out before they can be used effectively. It would also require a very significant investment of time and effort to capture the risks and relevant responses throughout a major bank. However, without this level of data, it is hard to envisage how more comprehensive risk programs might operate to the maximum potential benefit of the organisations and society as a whole. The level of granularity that would be required would also be a subjective matter in that while there might be an appropriate response to a high level risk, there may well be sub-risks that require a different response.

628 **RECOMMENDATION: In view of the complexity of this area, the international banking regulators should be asked to explore appropriate mechanisms for recording and aggregating risks and responses, which would then facilitate better risk sharing between organisations and with banking regulators and supervisors. It is possible that risk information provided to regulators in XBRL (eXtensible Business Reporting Language), using a common risk taxonomy, could well form the basis of this approach.**

Risk appetite

629 There has been a lot of discussion in the interviews for this paper, and also in the press and various inquiries about risk appetite. The more this issue is probed, the harder it is to get to grips with it. However, what is clear is that for different types of risk at different levels of the organisation, there are different risk appetites. There is a different risk appetite for risks that a company wishes to engage with, compared to the risk appetite for risks that represent pitfalls. While it might be possible to determine a risk appetite for certain types of risk that are subject to quantitative measurement, or for clear cut issues (for example the death of employees through accidents at work

would be intolerable for all banks) it is clear that there are other types of risk for which it is almost impossible to set an appetite.

630 It might be possible to begin to disaggregate risk appetite by looking at two of the principal components of risk appetite which are:

- The propensity to take risk; and
- The propensity of the organisation to exercise control.

In turn these two elements will be informed as much by the culture and processes of risk management and internal control as they will by explicit policies and statements of risk appetite. They will also be determined to a large extent by the organisation's performance culture (often significantly driven by its remuneration policies) and its corporate ethics and behaviours.

631 It is also worth noting that the risk appetite for one risk might be at variance with the risk appetite for another risk. Until there is greater clarity of the taxonomy and aggregation of risks referred to above, it is unlikely that we will be able to arrive at a sensible body of guidance on the issue of risk appetite.

632 **RECOMMENDATION: The international banking regulators should be encouraged to invest in research into practical ways of understanding, measuring and monitoring risk appetite. This is currently a long way from fruition.**

The importance of avoiding pitfalls

633 As already discussed, the prime motivating factors in determining a bank's approach to risk appear to be the nature of the industry, pressures from investors and the way in which the "irrational exuberance" of the markets can encourage all institutions to seek ever more levels of risky instruments (without always recognising the level of risk being assumed), or engage in more audacious acquisitions. The susceptibility of many banking risks to quantitative techniques also allows for the illusion of measuring residual downside risk. In practice it appears that banks probably have not spent sufficient time exploring the nature and management of downside risks, which can have a significant potential to destroy shareholder value (referred to elsewhere in this paper as pitfalls).

634 It is naturally difficult to persuade bankers in the midst of a long run bull market to stop, pause and think about the downsides of their actions. However, those organisations that do not assess the pitfalls that can pull the organisation up short are likely to suffer dire consequences. In a culture where growth, risk taking and aggressive tactics are applauded, being the individual who stops the organisation in its tracks can be very unpopular, as demonstrated by the HBOS whistle-blower, and his former colleague, both of whom have made much of a culture that did not like to hear bad news.

635 The sense from the interviews for this paper is that while banks pay lip-service to downside risk management and avoiding pitfalls, in fact there is a sentiment that the capital cushion will protect them. With the current Financial Crisis, we have seen that this is not necessarily the case. Whereas regulators may well encourage banks to undertake scenario stress testing, this should be

extended to cover a wide range of strategic and other risks which might not be traditionally examined under normal stress testing.

636 **RECOMMENDATION: Non-executive directors should play a key role in stress-testing the bank, its long term strategy and other strategic risks. This is not to dampen the entrepreneurial spirit, but rather to ensure that risk taking is done in a proportionate and managed way.**

The relevance of ethics to risk management

637 This paper has addressed extensively the risk culture of the organisation. Without a guiding sense of purpose, it is likely that the pressures from investors and the opportunities for breathtaking rewards will lead to increasingly morally questionable behaviours. While laws may or may not be broken, ethics come into play when considering behaviours that are not governed by laws but where "guiderails" are needed to assist in interactions between members of staff, with suppliers, customers and the public at large.

638 Ethics programmes are much more common in the US, probably encouraged by the US Federal Sentencing Guidelines which set out a framework for organisations which will be taken into account should a corporation be subject to criminal prosecution. By following the guidance of the Sentencing Guidelines, it is possible for companies to reduce the potential penalties in criminal prosecutions by as much as 95%.

639 What is interesting about the Federal Sentencing Guidelines is that, unlike many US rules, where we are used to black letter prescription, the Guidelines are just that: guidelines. They do not set out rules, they rather set out the sorts of things that you should do. The benefits are two-fold: (i) more lenient sentencing, should a matter get to that stage; but (ii) more importantly, preferential treatment afforded by Department of Justice (the "DoJ") in deciding whether or not to prosecute on a given set of facts.

640 In essence the Guidelines set out to encourage ethical corporate behaviour and reward those companies that take active steps to develop an ethical compliance programme and punish those that disregard the ethics of their business activities. So two companies that commit the same violation of the same law, the first has implemented an effective ethical programme and the second has not. The first may benefit from the leniency often applied by the DoJ in practice using the "effective" compliance programme Sentencing Guidelines approach, the second runs the real risk of having the full weight of the law thrown at them.

641 In a society that prides itself on its "ethical" approach to life (the inventors of cricket and the Marquis of Queensbury Rules for boxing) it is a strange contrast, in the UK, that ethical policies tend to be set by the legislative process and potentially by purchasing practices in the public sector. For example, most large companies now have an equality or diversity policy, they are increasingly developing anti-bullying programmes and so on. These are largely driven by societal changes dictated at national level, rather than by a preference to act in a morally or ethically appropriate manner.

642 However, this area is important. Surveys in the US have shown that a significant proportion of staff, when questioned, have seen acts or behaviours that are inappropriate within the organisation, and which, were they disclosed to the public could result in material damage to the

reputation of the organisation. However, on further questioning, approximately 50% of those staff would not do anything about it, either because the organisation simply would not take the accusation seriously, or because it could actively harm their career. Equally, a significant proportion of staff would not bother to tell management about improvements that could be made to activities, products or processes on the basis that they would be stepping on someone's toes in a much more senior role and therefore they would suffer severe detrimental consequences in their careers.

643 It is not difficult intellectually to extrapolate from the ethics of the question to the risk management ramifications. Ethics needs to be more than simple legal compliance with local laws and regulations (as presupposed in the first COSO framework on internal control). It also needs to be about the moral compass that guides each member of staff in the context of the organisation's business.

644 **RECOMMENDATION: Each board should formally review the ethics programme of their institution on a regular basis and should take regular soundings to ensure that it remains effective. Directors should take steps to ensure that the "dangerous silence" is addressed so that individuals can raise appropriate and reasonable grievances or concerns in a manner which is not harmful to their personal well-being. This potentially goes much further than traditional whistle-blowing programmes. In addition, boards need to take action to ensure that their organisation is living up to the ethical values they have chosen so they should have full programmes that include not just communication but training, discussion, reporting and leading by example.**

645 It is worth noting that anthropologists argue that there is a maximum size of unit for effective communications. While the exact size is debated, the upper limit is somewhere in the region of 150 people. Given the size and complexity of the global banks, it is important that boards of directors take responsibility for ensuring that there are appropriate communication lines for the purposes of engendering a deeply held sense of ethical behaviour in the organisation.

The extended enterprise

646 Risk management is complicated even when looked at simply within the boundaries of an organisation. The efficiency of risk management in a traditional economic unit, an enterprise, is dependent on the skills of management in fostering and managing the risk management programme. However, where traditional boundaries become semi-permeable through alliances, joint ventures and outsourcing, the relationship between objective, risk and response is broken where a third party takes on responsibility for a part of the risk management chain.

647 It is often assumed that outsourcing exports risks. Outsourcing can, however, frequently produce risk importing through risk dependency. Where the linkages are broken and Company A is responsible for the objective, but Company B manages the likelihood and timing of achieving those objectives (because it manages the risks or the risk responses), then this gives rise to the dependency risk conundrum: who is managing what? For whom? And why? And how?

648 Exactly the same issues arise whether we are talking about alliances, joint ventures or outsourcing: the complicating factor is the number of parties to the relationship. The more there are, the harder it becomes to exercise control. Traditional responses, many of which remain valid, even in today's world of virtual and real joint ventures and alliances include:

- Good definition of the scope of the JV, respective responsibilities, and appropriate management;
- Good legal documentation; and
- Appropriate insurance cover.

649 But these all have shortcomings: the management route is orders of magnitude more difficult to pursue. Needless to say, legal documentation should only be relied upon as a last resort: where the objectives of a JV and its operation have broken down. Insurance is a "sticking plaster" approach to management in that it deals with the symptoms of problems, but not the root causes. Consequently there are new approaches that need to be called on in order to ensure that the extended enterprise can work:

- Build trust – both internally and externally;
- Share risk management data – between participants to the relationship; and
- Create a partnership of risk intelligent organisations.

650 Essentially, the answer is to create a risk intelligent partnership, which implies the creative collaboration of two or more risk intelligent organisations, supported by the flow of risk data in a format that can be digested and utilised by all parties.

651 Historically joint ventures have often been used in the belief that risks are being mitigated. However, the world is littered with failed joint ventures. This is in part because managers are often blind to dependency risk and because they settle for a reactive approach to risk management. The solution is to work with a new resolve towards the creation of "risk intelligent partnerships". The hallmarks of a risk intelligent partnership are:

- Trust, both between partners and also between the joint venture and the customer;
- Achievement of objectives; and
- Better satisfied customers.

652 Given the complexities of modern global financial services, there is an increasing use of alliances; accordingly, this area of the extended enterprise is important. Equally, as we have seen through the current Financial Crisis, irrespective of the more formal alliance relationships, banks are entirely dependent upon one another for liquidity. It is therefore in the interests of the Banking Regulators and Supervisors to ensure that shared risks are properly managed across organisational boundaries.

653 **RECOMMENDATION: The International Banking Supervisors and Regulators should explore mechanisms for sharing risk data between participating banks where risks cross organisational boundaries. In this regard there may be an opportunity to leverage the work referred to earlier about risk taxonomies and the use of a risk variant of XBRL.**

VII An assurance framework

701 Section IV describes a distressed model of Corporate Governance. To recap:

- Corporate Governance is (almost) voluntary;
- Investor pressures are fierce, leading many businesses to undertake risks that simply are not in the best interests of the organisation;
- Non-executive oversight is stretched in that directors only have a limited amount of time to devote to the organisation, but almost unlimited responsibilities;
- External audit is stretched to a point where the degree of reliance that is placed upon it is out of proportion to the amount of work that actually goes into it;
- Internal audit is struggling, largely because many internal auditors are not the beneficiaries of the regard that they are owed;
- Obtaining assurance from regulators, financial analysts and rating agencies cannot be comprehensive;
- Which leaves boards with dependence on management including the risk management team, and General Counsel (or the Company Secretary).

702 Section V outlines proposals for a new duty for boards to discharge their Corporate Governance responsibilities with due and diligent care. This would help to enforce a change of culture that is engrained in the Banking industry, (and in others) an industry which contributes significantly to the proper functioning of our economic system.

703 Section VI describes a balanced approach to risk management that addresses the pitfalls and the ethics as much as the risk taking and the performance culture; that encompasses the totality of the risk universe, both within the organisational boundaries and across semi-permeable boundaries.

704 All of this requires an oversight, or assurance approach that can act as a counter-balance to the naturally entrepreneurial inclinations of the CEO and management. This is not to act as a bureaucracy or serve to chill the essential entrepreneurial spirit of management. Rather it is in recognition of the major societal impact that these major financial institutions have when they face problems such as those that have emerged in the current Financial Crisis. These banking institutions owe a responsibility to society that is greater than that of most other organisations. They are so important to our societies and to the global economy at large that they cannot be allowed to fail: they are “too big to fail”.

705 With this in mind, it is worth cautioning that there is no “one-size-fits-all” approach to improving the assurance received by, and dispensed by boards. Accordingly, this section sets out a range of possible improvements that could be made to board assurance processes.

Risk management and assurance framework

706 Section VI sets out a vision for a comprehensive risk management framework which would address the totality of the risk universe (down to an appropriate level of granularity) both inside and outside the organisation. This envisages that management should operate within that risk management framework, and that a properly funded and staffed group should act as guardians of the risk management framework. While the internal audit group should continue to carry out its

function to review the operation of the risk management framework, including the effectiveness of reporting to the highest levels, and the continuing operation of appropriate risk responses. The internal auditors should work with the risk management group to ensure that there is a single view of risk management.

Documented assurance map

707 At the moment, there is a sense in which assurance simply happens. It is not a planned activity in the way in which parts of it are executed: for example most internal audit departments normally prepare an annual plan which is presented to and discussed with the Audit Committee. However, there is rarely an overall, documented plan for the totality of assurance that is required at board level and which the board needs to provide to other stakeholders.

708 In order to assess the requirements for resources and funding for assurance purposes, the board should annually prepare or update an assurance map which should as a minimum:

- Document the people to whom assurance is required to be provided (eg regulators, investors, customers and so on), the nature of the assurance, how that assurance is to be provided and how the board is going to satisfy itself that the assurance that is being provided is truthful, correct and appropriate in all the circumstances.
- Document the manner in which the board will seek and obtain assurance that what they are told is happening in respect of the business is indeed happening in order to discharge the assurance aspects of their Corporate Governance duties to exercise risk management oversight.
- Document the way in which the board is assessing, monitoring and managing the risk management culture, and progress towards becoming a risk intelligent organisation

709 **RECOMMENDATION: The board should develop an assurance map which should be updated regularly as events dictate, but no less that at least annually.**

Risk management group

710 The risk management group should have unfettered access directly to the board, reporting either to the Chairman (if the roles of Chairman and CEO are split) or to the Chair of the Audit or Risk Committee (if the CEO and Chairman roles are not split). The budget for the group should be set by the board member responsible for the direct report, not by the CEO or the CFO. The sponsoring board member should be responsible for senior recruitment decisions and for terminating employment. Any decision to terminate the employment should be accompanied by a letter from the role holder to the board stating whether or not there are any circumstances that the individual wishes to bring to the attention of the board.

711 The head of the risk management group should not be remunerated by reference to the financial success or otherwise of the organisation, but rather should be remunerated by reference to objectives agreed between the role holder and the sponsoring board member.

712 The risk management group should be tasked with determining risk management policy, in conjunction with the board, assessing and reviewing the risk management culture and the risk maturity of the organisation. They should provide the mechanisms for identifying, assessing, managing and recording risks and the necessary IT infrastructure.

713 There is no reason why the risk management group should not be a good career development route for people in other parts of the business. However, it might also be some individuals' preference to remain entirely within a risk management group.

714 The head of the risk management group should report to the board on a regular basis, and have the absolute freedom to seek access to any member of management and any non-executive member of the board. Going to the Chairman should not be seen as the "nuclear" option.

715 **RECOMMENDATION: There should be a risk management group or function, headed by a senior individual with direct access to the board. This individual should be responsible for all aspects of the risk framework throughout the bank.**

Internal audit

716 This paper does not propose any significant change to the role of internal audit. What follows would probably be familiar to most heads of internal audit. However, it is set out here for the sake of completeness.

717 Internal audit's primary responsibility should be to ensure that the risk management approach is being followed throughout the group, and that appropriate internal controls are in place and are operating effectively. They should work on a risk-based audit plan that seeks to deliver assurance to the board as to the efficacy and efficiency of the risk management approaches adopted, including of the framework as a whole.

718 In common with the risk management group, the internal audit group should have unfettered access directly to the board, reporting either to the Chairman (if the roles of Chairman and CEO are split) or to the Chair of the Audit Committee (if the CEO and Chairman roles are not split). The budget for the group should be set by the board member responsible for the direct report, not by the CEO or the CFO. The sponsoring board member should be responsible for senior recruitment decisions and for terminating employment. Any decision to terminate the employment should be accompanied by a letter from the role holder to the board stating whether or not there are any circumstances that the individual wishes to bring to the attention of the board.

719 The head of internal audit should not be remunerated by reference to the financial success or otherwise of the organisation, but rather should be remunerated by reference to objectives agreed between the role holder and the sponsoring board member.

720 There is no reason why the internal audit group should not be a good career development route for people in other parts of the business. However, it might also be some individuals' preference to remain entirely within an internal audit group.

721 The head of internal audit should report to the board on a regular basis, and have the absolute freedom to seek access to any member of management and any non-executive member of the board. Going to the Chairman should not be seen as the "nuclear" option. The head of internal audit and the sponsoring board member should share a responsibility to build a real and effective relationship between the head of audit and the board to create trust and understanding.

722 **RECOMMENDATION: All boards should review their internal audit departments to ensure that they are appropriately resourced, headed by a heavy weight individual with access to the board, and that they are adequately funded. Management should not be empowered to impose restrictions on the internal audit department.**

Other key assurance role holders

723 The board should ensure that they have unfettered access to any other key assurance providers as needed: for example compliance officers, ethics officers and other similar assurance providers. The board should ensure that they have the full details of reporting lines, that they monitor budgets for these role holders and are kept informed of any changes in the role holders.

724 **RECOMMENDATION: All boards should prepare a schedule of key assurance role holders, and that they should ensure that these role holders and their teams are appropriately resourced and funded and report independently of management to the board on a regular basis.**

External assurance

725 To the extent that the assurance map determines that the board will have to place reliance on outside suppliers (for example the external auditors, or outsourced internal audit providers), they should ensure that the providers are independent, are appointed by them and have a direct reporting line without interference from executive management.

Chief Assurance Officer or Director of Risk Management and Assurance

726 While one or two interviewees have dissented from this view, the majority have been of the opinion that it would be appropriate to have a very senior individual overseeing the risk management and assurance framework. Where there is a mix of executive and non-executive members of the board (the UK and French model) then it would be appropriate for that individual to be on the board.

727 Where there is a predominantly non-executive board (the US model) then it might be sufficient for the CAO to be a member of the "C-Suite", although there would be an expectation that the individual would regularly be in attendance at board meetings.

728 Any individual filling the role of CAO or Director of Risk Management and Assurance would have to be independent of mind, sometimes referred to as "objectivity of thinking". Their independence would be supported by the appointments process and the reporting lines. They would be appointed by the board as a whole (perhaps through the nominations committee, or under the auspices of the Audit Committee) and any termination of their employment would be a matter for the entire board, with the same requirement to circulate a letter confirming whether or not there were any matters they wished to bring to the attention of the board on termination of their employment.

729 In common with the head of risk management and the head of internal audit, remuneration should be based not on the financial success or otherwise of the organisation, but rather by reference to objectives agreed between the individual and the Audit Committee.

730 **RECOMMENDATION: All boards should consider the appointment of a Chief Assurance Officer or Director of Risk Management and Assurance, and consideration should be given to appointing this individual to the board, and ensuring that they have the appropriate status in the organisation, reporting directly to the Chairman (where the roles of Chairman and Chief executive are split) or otherwise to the Chair of the Audit Committee. Where such an individual is appointed, the Head of Internal Audit and the Head of Risk Management should report directly to them, as well as having an open line into the board room.**

Full time non executive directors

731 Especially where there is either no CAO (or equivalent), or the role holder is not on the board, the board should consider the appointment of one or more full time non-executive directors to oversee the risk management and assurance framework. The work of audit committee members is already onerous and hard to discharge as a part time role, and this would only be more so in the context of the work that would be involved in establishing a fully functioning risk management and assurance framework as envisaged by this paper.

732 **RECOMMENDATION: The banking regulators and supervisors should consider encouraging, or in some cases where the societal duties require it, instructing boards to appoint full time non-executive directors to act as an effective counter balance to the executive management.**

733 Some might argue that full time non-executive directors become de facto members of the management team. Their purpose would be to ensure that all aspects of the risk management and assurance framework operate effectively. They would have to develop a proper and effective working relationship with the CEO and other executive officers, but they would report to the Chairman of the Board (where the roles of Chairman and CEO are split) or to the Chairman of the Audit Committee. Their remuneration should be based not on the financial success or otherwise of the organisation, but rather by reference to objectives agreed between the individual directors and the Remuneration Committee.

Governance audits

734 Boards should seek independent reviews of their governance arrangements, in particular they should:

- Obtain independent reviews of the board's and board committees' performance, rather than conducting the reviews themselves;
- Commission a periodic (at least once every other year) review of their risk management and assurance framework and of their assurance map. The review should focus on the scope and coverage of the framework, the review of the risk culture and the scope and nature of the work of the risk management group, internal audit and other assurance providers.
- Commission a periodic (at least once every other year) review of the other corporate governance arrangements, to ensure that they remain fit for purpose and consistent with best practice in the industry.

735 These reviews should be commissioned by and report to the independent non-executive directors.

736 **RECOMMENDATION: Banking regulators and supervisors should require banks to commission periodic governance audits as outlined above. Such audits should be carried out be an independent organisation and should not be conducted by the current external auditors.**

Appendix A – Terms of Reference

The terms of reference for this paper are set out below:

> "To submit a substantial report on corporate risk-management; the link between risk management strategies and remuneration policies, and; the role of the board of directors in establishing and monitoring risk management strategies and remuneration policies.
>
> "The report shall be based on a survey of the experiences with existing risk management standards, including, but not necessarily limited to, those in France, UK and the US. The report shall describe how the standards relate to the overall corporate governance framework and provide an overview of how they are monitored, implemented and enforced in practice. Possible weaknesses in these respects and the origins of such weaknesses shall be identified and analysed with a view to any public policy implications. Special consideration shall be given to the *interplay* between risk management, remuneration and the role of the board of directors.
>
> "When identifying possible causes for weak implementation, the report shall also analyse if there are "legitimate" firm-level constraints and conditions that render certain parts of standards unnecessarily ineffective or impractical. By using examples, this analysis shall form the basis for proposals on how risk management standards, in principle, can be made as effective as possible in terms of their content, monitoring and firm level implementation. The relationship between risk management and internal controls relating to financial reporting shall also be addressed in this context.
>
> "This research will enable some of the hypotheses put forward in the letter to the Deputy Directors to be considered and either supported or rejected in the final write up.
>
> The report will provide input to the work of the OECD Steering Group on Corporate Governance and the OECD Strategic Response to the Financial and Economic Crisis."

Appendix B – Interviewees

Jackie Cain	IIA UK
George Dallas	F&C Management Ltd
Simon D'Arcy	IIA UK
Sir Howard Davies	London School of Economics and Political Science
Odile de Brosses	Association Française des Entreprises Privées
Claudio Domenick	SOX and Financial Controls Expert
Gary Edwards	Ethos International
Richard Gossage	Lloyds Banking Group
Holly Gregory	Weil, Gotshal & Manges LLP
Chris Hodge	Financial Reporting Council
Sir Christopher Hogg	Financial Reporting Council
Dr Thomas Huertas	Financial Services Authority
Alexandra Lajoux	National Association of Corporate Directors
Lester A Myers	Independent Consultant
Professor Mike Power	London School of Economics and Political Science
Dan Roberts	RAAS Consulting
Christian Schricke	Société Générale
Keith Smith	Strategic Thought
David Styles	BERR
Dan Swanson	Independent Consultant
Arnaud Vigne	Independent Consultant
John Webb	IIA UK Banking & Finance Sector Internal Audit Group

In addition, some interviewees preferred to remain anonymous.

I would particularly like to thank Jackie Cain, Richard Gossage, Chris Hodge, Tom Huertas, Alexandra Lajoux. Dan Roberts, Keith Smith and Dan Swanson for commenting on earlier drafts of this report. Any errors remain mine.

Appendix C – Balanced Risk and Dimensional Control

This appendix provides a brief overview of two approaches to risk management that have been developed to deal with some of the issues referred to in the body of the report. The concepts behind balanced risk are derived from a benchmarking exercise of five non financial services FTSE100 companies carried out by the author. The second approach, known as Dimensional Control, was developed by Professor Robert Baldwin of the London School of Economics and refined by him and the author in the course of consulting engagements.

Balanced risk

The body of the report refers to Balanced Risk. The underlying concept is set out in this appendix. It has been kept separate from the body of the report because others may well see the issues in a different light or use an equally appropriate, but different model.

The argument runs that organisations engage with risk at a corporate level in four different ways:

- Companies have to take more managed risk ("MMR") if they are to continue to grow and develop;
- They also have to avoid pitfalls ("AP") if they are not to destroy shareholder value. These two approaches are potentially in tension since they require different management skills.
- The third risk engagement is by means of the performance culture ("PC"). In the case of the banking sector, this has been driven by bonuses often paid out on the back of short term results rather than sustained performance. In other organisations the performance culture may be driven by other factors: for example the desire to work for the good of society, or in pursuit of pure knowledge.
- The performance culture is often in tension with corporate ethics and behaviours ("CEB").

In each case, the stronger the attribute the better the long term performance, until you get to the stage where diminishing returns or indeed negative returns begin to accrue:

- The company pursues MMR to the extent that it can no longer cope with increasing initiatives and new risks become unmanageable;
- The company spends all of its time avoiding pitfalls to the extent that it starts to become totally risk averse;
- The performance culture becomes so demanding that people begin to break rules and they suffer from burnout; and
- Corporate ethics become so intense that the organisation starts to suffer from "egg shell" syndrome.

This is shown in Figure 3 below:

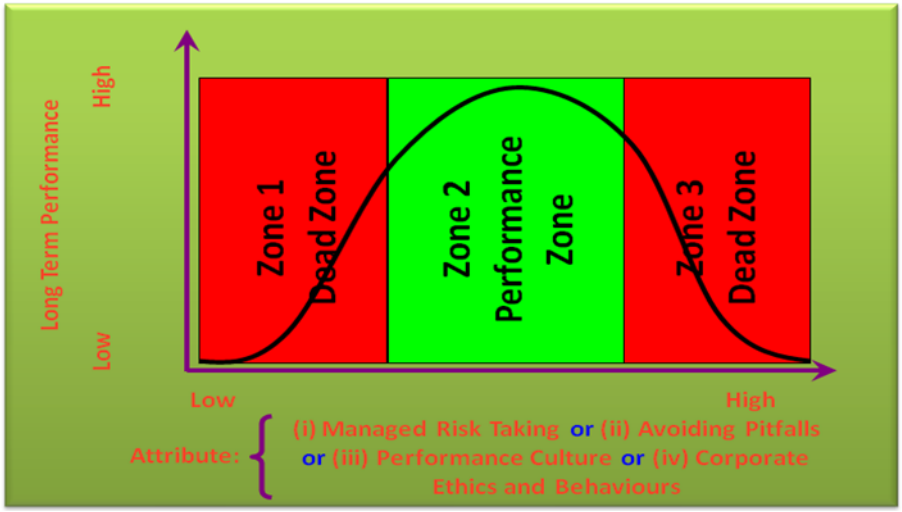

Figure 3: Long term performance against risk attributes

Mapping all four attributes on the same diagram, with the axes going from little to lots, produces a diagram as shown in Figure 4 below:

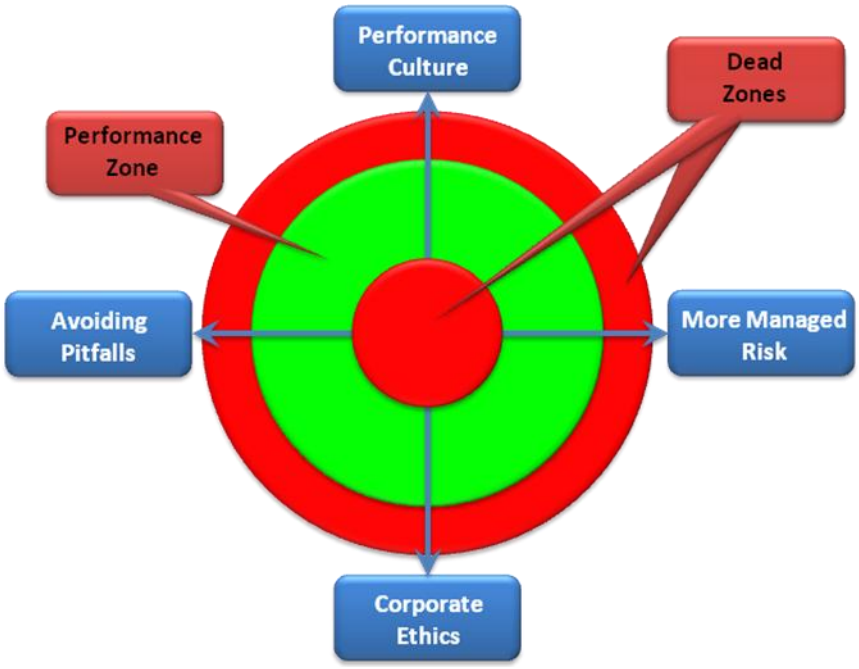

Figure 4: All four attributes with axes from little to lots

It can be argued that many of the banks took too much managed risk, and they clearly had demanding performance cultures. However their ability to avoid pitfalls was insufficiently developed as was their corporate ethics. This results in a diagram as set out in Figure 5:

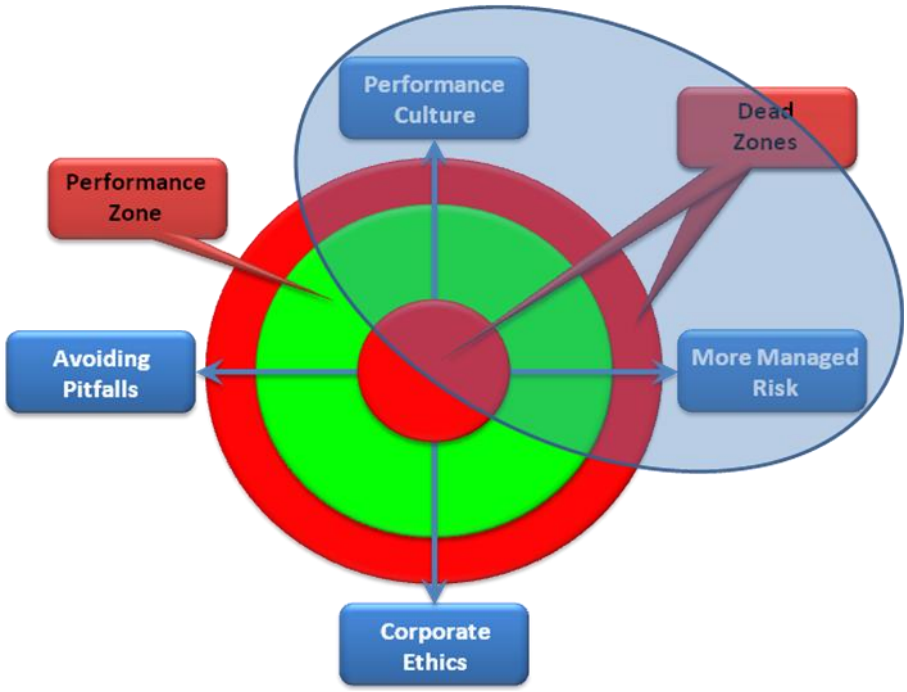

Figure 5: A banking industry risk management profile

This is the risk management profile that has brought the banking industry to its knees in the current Financial Crisis. On the other hand, many people might argue that the normal profile for UK companies is as follows:

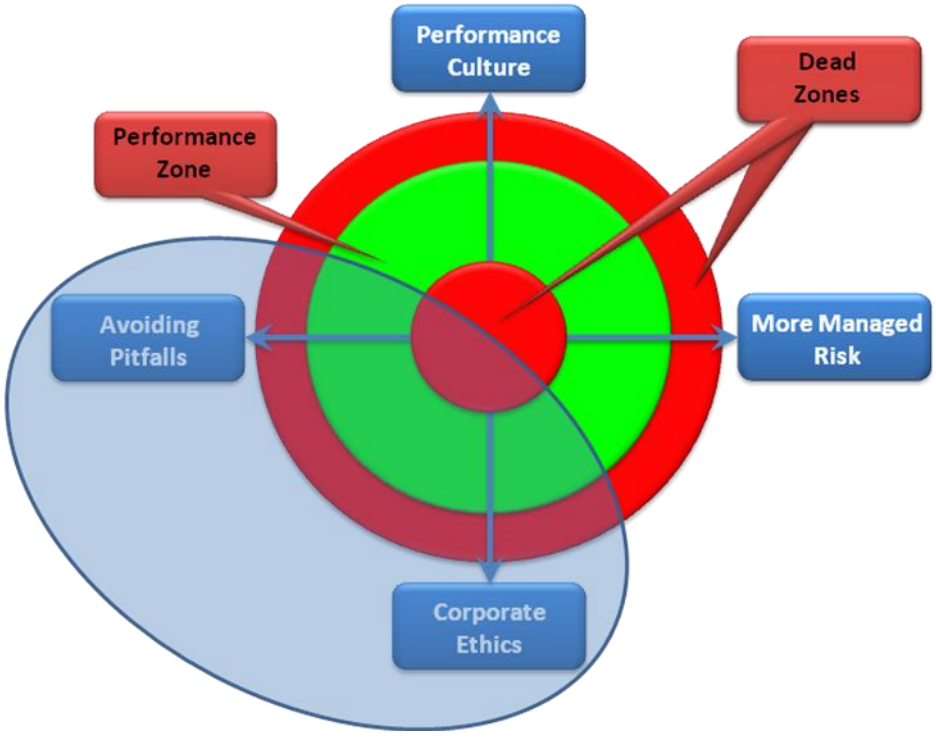

Figure 6: UK plc risk management profile

With the clear exception of the banking industry, UK plc is good at avoiding pitfalls, after all there are many regulators who are prodding companies to avoid pitfalls. UK plc is thought to have good

corporate ethics (the British invented cricket and the Marquis of Queensbury Rules), but the markets are not overly keen on more risk and the newspapers positively berate any signs of performance.

The objective of risk management should be to identify the extent of the green, or performance zone, to maximise it and to ensure that the organisation does not become caught in the red, or dead zones as shown in Figure 7

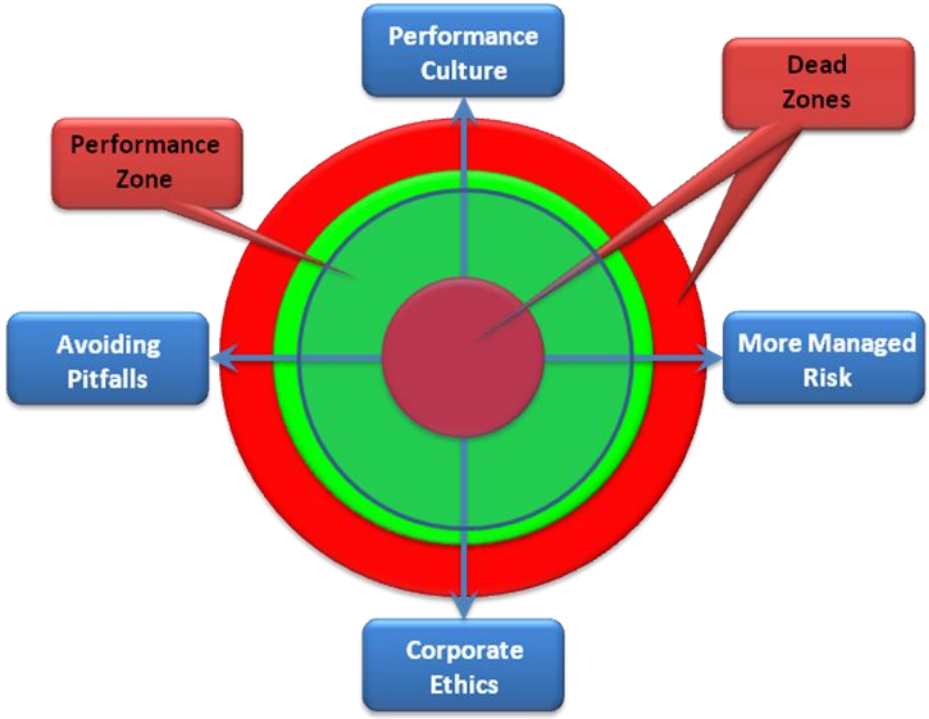

Figure 7: Balanced risk management

The objective of many of the recommendations in this report is to encourage organisations to establish the balance shown in Figure 7, and then to ensure that it is retained within the operations of the organisation through the risk management and assurance framework.

Dimensional control

Dimensional control is an approach to developing or assessing risk responses by looking at the five dimensions of control, which are:

- **Strategy**: by which we mean do you want to prevent a risk from happening or allow it to happen and deal with the consequences, by, for example devising an appropriate contingency or disaster recovery plan.
- **People**: by which we mean do you want the risk to be managed by specific individuals, or is it something that needs to be managed throughout the organisation.
- **Detail**: by which we mean do you want to manage general risks or specific risks.
- **Tasks**: by which we mean the activities of gathering information, devising plans, procedures or approaches to managing the risk and then the actions, including implementing the plans, and looking for assurance that the proposed action has been taken.

- **Drivers**: by which we are referring to the need for someone or something to make sure that the whole process takes place. These drivers include managers in the organisation, outside regulators or the culture of the organisation.

This is shown in Figure 8 below:

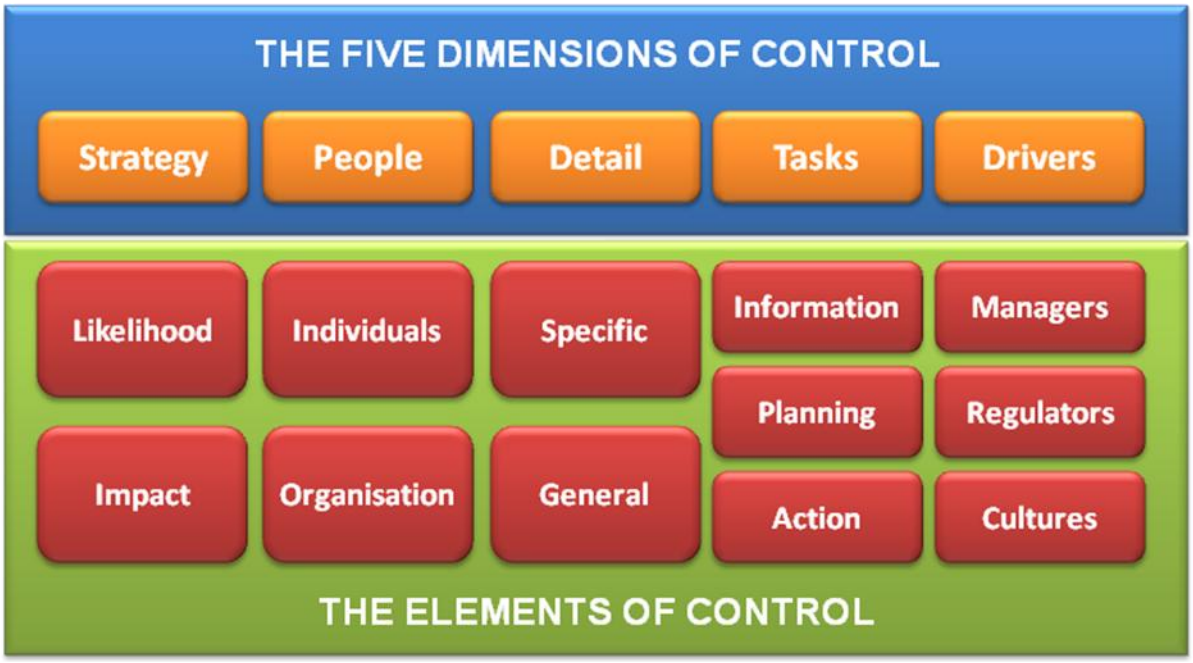

Figure 8: Dimensional control

By understanding the rationale for engaging with a risk as set out in the section above on balanced risk, and then determining which of the elements of control are required to ensure that the appropriate response is achieved, companies can ensure that their risk response is consistent with their strategy and in line with their risk appetite.