THE ICAEW FOUNDATION

INDEPENDENT AUDIT LIMITED

# GETTING IT RIGHT

## A REPORT BY INDEPENDENT AUDIT LIMITED ON RISK GOVERNANCE IN NON-FINANCIAL SERVICES COMPANIES

## OCTOBER 2009

Inside front cover is blank

# FOREWORD

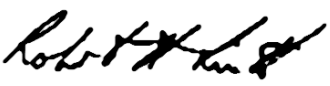
Crises provoke fears of heavy-handed regulation following in their wake. The extreme situation in the financial markets over the past two years has, quite rightly, led to questioning of the effectiveness of our governance approach. Thorough reviews by the Financial Reporting Council and by Sir David Walker are resulting in proposals for changes to the Combined Code. As we debate proposals, we must make sure they are justified by evidence on where weaknesses lie, and are supportable as pragmatic and effective solutions.

This report is a very welcome addition to the body of evidence which must be considered. The ICAEW Foundation is to be applauded on taking the initiative to undertake more detailed research in this area. Although changes to the Code must have approaches to the governance of risk as a primary focus, the debate has, until now, been hampered by a lack of current evidence on what non-financial services company boards and senior management are actually doing to oversee risk-taking and risk management. In covering about a quarter of the non-financial institutions in the FTSE 350, this report from Independent Audit successfully helps to plug that gap. It gives us a clear picture of existing practice to help us make sound judgements on what, if anything, needs to change.

The results are reassuring but must not lead to complacency. Practice in the companies covered by the research suggests that boards and management have, over the past few years, put considerable effort into strengthening risk identification processes and making sure that board committees are putting the time into overseeing risk management. Boards have become much more aware of the need to obtain a clear picture of the risks the business is facing, to understand the quality of management's response and to have a real debate on how much risk to take. Top management have recognised the need to take the lead and hold their teams accountable. This progress needs to be sustained and the good practice maintained, making sure that the commitment to get risk management right is not overcome by a box-ticking mentality or a more relaxed approach as we move into an economic upswing.

The picture of good practice presented in this report does not necessarily extend to the companies which did not participate (I suggest to them that it is a good point of reference to check themselves against). So we must not assume that this sample, albeit a large one, means that the situation is universally and consistently healthy – common sense tells us it won't be. And the key message – that good risk oversight comes down to the right behaviour, not just process – means that we have to be constantly vigilant to make sure that we are all behaving in the right way. Boards need to be challenging and debating continuously; CEOs need to be showing leadership and keeping the board in the picture at all times; and management teams need to be making sure that risk management is simply part of day-to-day management and reporting transparently on the real risk positions.

The picture presented by this extensive research suggests that we need to concentrate on making our present system of governance work well, not on adding more regulation or process. If this is where the debate settles, most will, I suspect, breathe a sigh of relief. But we can't let it be a sigh of contentment or of relaxation. Getting this right requires continuous commitment and hard work.



**The Lord Smith of Kelvin**

# CONTENTS

# HIGHLIGHTS

The Combined Code's principles regarding risk governance remain valid and there is no case for significant change in the UK's approach to regulating governance. Improving risk governance means improving the way in which the Code's principles are put into practice. This is primarily a responsibility of boards of directors, but there are opportunities for regulation to help them by clarifying or re-emphasising what the Code is trying to achieve.

The situation to be dealt with by risk governance in corporates is significantly different from that in financial services organisations. The nature of many of the risks, the way in which risk management structure and process have evolved, and the role risk management and measurement play in regulation are distinctively different. Structural or process solutions that are thought to be appropriate for financial services organisations should not be presumed to be suitable for corporates.

Boards have two main responsibilities in relation to risk. One is to determine and communicate to the organisation what constitutes acceptable risk-taking. This is done in a number of ways: through the board's explicit acceptance and rejection of major risks, by requiring a degree of resilience to cope with the unexpected, and through expressing a consistent attitude to risk and control. All are so fundamental to a director's duties that they should normally be a matter for the entire board.

The other main responsibility is to oversee the management processes for the identification, assessment and mitigation of risk across the organisation. This is something that can reasonably be delegated to a committee. The audit committee is usually well-placed to do this and there is rarely a critical need for a separate risk committee of the board. Some do find it useful to use separate committees for dealing with specific classes of risk that require special attention, but this is a practical solution for particular circumstances and not something to be mandated.

Effective risk governance, and corporate governance more generally, rest primarily on human behaviour. New rules, or even new principles, are not what is needed to make risk governance more effective. What is needed is for people to make a good job of living up to those we already have.

Some of the recommendations in the Walker Review are aimed at reinforcing awareness of this and are equally relevant to all companies, whether financial services or not. Chief among these are recommendations aimed at ensuring boards make proper use of performance evaluations to challenge their own performance.

There are opportunities to improve the Combined Code in order to emphasise or clarify how principles should be put into practice. These affect, for example:

- the role and responsibility of the board, committees and individual directors regarding risk acceptance and oversight of risk management processes;
- the *Turnbull Guidance on Internal Controls*, which seems more than usually prone to box-ticking implementation;
- the importance of non-executive directors (NEDs) being fully engaged in the business, without straying into executive territory;
- indicators of non-executive director independence, balanced against the increased effectiveness that comes from the knowledge acquired over a long term of office;
- the need for boards to give attention to, and receive information and assurance on, values, attitudes and other behavioural matters; and
- the breadth of experience and expertise around the board table, and in particular ensuring that audit committees possess the non-financial expertise necessary for effective risk oversight in their own circumstances.

# GETTING IT RIGHT

Risk management, and the governance of it by boards of directors, is receiving a lot of attention at present. It may be helpful to begin this report with a reminder that the purpose of risk management is not to prevent things ever going wrong. Equity rewards are achieved through taking risk, and when risk is taken then there will sometimes be losses. The purpose of risk management is not to ensure that no risks are taken and no losses ever incurred, but that risks are not taken unknowingly or recklessly. In real life, of course, this is unlikely ever to be fully achieved, but it is the goal towards which risk management should be working.

The recent banking crisis has exposed some banks in which risks were taken unknowingly or recklessly, and on a grand scale at that. Consequently, various proposals to improve risk management in banks and other financial institutions have been made, most notably in the Walker Review.[1] The Walker Review makes a number of recommendations relating to, among other things, the governance of risk, the functioning of the board, and board composition and qualification. While some of its recommendations are self-evidently specific to financial services organisations, others would be capable of more universal application.

Independent Audit Limited was asked to investigate the practice of risk governance by the boards of non-financial services companies, with the aim of obtaining evidence on whether it would be helpful to extend some or all of the Walker Review recommendations to companies which are not primarily engaged in financial services. The evidence obtained, and the scope of investigation on which it is based (the review included a large number of interviews as well as a questionnaire-based survey) are set out in this report.

We found clear differences between financial services organisations and corporates,[2] not only in the nature of their businesses and risk exposure but also in the role that risk management plays within the organisation. These differences mean that **the nature of the problem to be addressed by board governance of risk is different. Consequently, it should not be presumed that risk governance in corporates must be organised in the same way as in financial services organisations.**

Most importantly, while risk management has developed in financial services organisations to be a critical control and measurement function which has a significant part to play in the determination of regulatory capital, risk management in corporates has not taken on a life of its own in this way. In corporates, risk management is simply seen as an inseparable element of good business management, without the emphasis on quantification, and board governance of risk therefore seen as an inseparable part of holding management accountable.

Certain risk management techniques, such as risk reporting, are used to facilitate good management and board oversight, but the responsibility for these lies firmly with business management and not with functional specialists. There is a near-universal view, with which we concur, that **structural changes which could dilute the board's and the management's responsibility through establishing risk management as something distinct from business management, or risk governance as separate from overall board responsibility, are not merely unnecessary but would be positively unhelpful.** Unhelpful changes of this sort would include making board risk committees mandatory and requiring an independent Chief Risk Officer (CRO) to be involved at the highest level.

We were pleasantly surprised to find that, in our interviews with directors and officers of corporates for this study, the discussion would often and early turn to culture, values and ethics. There was a widespread understanding that good risk management, and good risk governance, were primarily about **human behaviour**. Structures and processes can help or hinder good behaviour, so it is a good idea to try and have ones which do more helping than hindering – but even well-designed structures and processes are not sufficient in themselves. Tone at the top, leadership by the CEO and chairman, being consistent in setting an example and communicating an attitude to risk, possessing the expertise and character to be able to challenge the executives – these are the board behaviours that form the foundation of good risk governance.

1 *A review of corporate governance in UK banks and other financial industry entities*, Sir David Walker, 16 July 2009.

2 A note on nomenclature: although some of those interviewed for this study referred to financial services organisations as 'BOFIs' (banks and other financial industry entities), there seemed to be a widespread feeling that the acronym, while convenient, is sadly inelegant and should be resisted. In this report, we therefore refer to non-BOFIs as 'companies' or 'corporates'.

Within the framework provided by the Combined Code, corporates have organised themselves in a variety of ways, all conforming to these principles. There is no single organisational model that stands out as promoting the right behaviour any better than others. A clear message emerges from the evidence presented in this report: **fundamentally, what's needed is not more rules, not even more principles, but for companies to make a good job of putting into practice those we already have.**

A number of the Walker Review recommendations relating to risk governance, and others relating to the overall effectiveness of boards, seek not to add to the provisions of the Combined Code but rather to emphasise **the importance of living in accordance with the Code's principles**. The evidence contained in this report suggests that it would do no harm for such emphasis to be extended to all companies covered by the Code.

The essential elements of good risk management include leadership by the CEO (again) and the senior executives; education and training of managers and staff; openness and the willingness to own up when things are going wrong; clear accountability backed up by a strong internal audit function. None of these things are new either. The key point is that to be effective they have to be done well, and they have to be maintained by the active involvement of management. And risk governance, if it is to be effective in its oversight of these activities, must look at their **quality, not compliance**.

But even the best managers, even when supported by world-class process, make the occasional mistake when foretelling the future. This is sadly inevitable – after all, if they could perfectly foretell the future, they wouldn't be working for a salary. It has been said that we can only be certain of death and taxes; risk managers might want to add the certainty that something unexpected will threaten to muck things up. So an essential part of good risk governance is not to rely too much on registers of identified risks, but to ensure that the company has sufficient **resilience**, both financial and operational, to withstand unexpected shocks. Recent experience has taught many companies that it's handy to have a comfortable margin for error.

There are two areas where **unclear terminology** creates scope for confusion. One is risk governance itself and the other is risk appetite.

'When I use a word,' Humpty Dumpty said, in rather a scornful tone, 'it means just what I choose it to mean – neither more nor less.' While Humpty Dumpty is perhaps not the best example of a good risk manager, he would undoubtedly have appreciated the term **risk governance**, which can be used to mean pretty much whatever suits you. Behind the expression there lie two distinct activities, and life becomes a little simpler if the distinction is maintained. One activity is board oversight of the risk management processes that exist across the company, either as indivisible elements of day-to-day business management or as separately identifiable facilitating processes. The other activity is in relation to risks which are individually significant at a group level, where the board goes beyond oversight and actively participates in the identification, assessment and acceptance of material risks.[3]

Both activities need to be done well if a board is to be fully appreciated by the executives. If a board is seen as being primarily engaged in oversight of risk processes, it is in danger of being seen by executives as a necessary overhead rather than as something which adds value.

**Risk appetite**, like many of the techniques of risk management, has its home in the financial services industry, where it has been interpreted to mean the financial quantification of acceptable risk exposure. Corporates well understand and appreciate the concept of 'acceptable' in relation to risk exposure, but struggle over giving it financial quantification. This is hardly surprising since so many of a corporate's risks are non-financial in nature, even if they will ultimately have financial consequences. 'Risk attitude' is a better descriptor of what most corporates understand to be useful, and in most corporates it is communicated to management implicitly, by inference from the board's decisions. It is in fact possible to communicate it more explicitly, using words rather than numbers, and some boards could do more to make their attitude to risk explicit. This would make it more consistently understood across the organisation, and therefore more likely to be followed.

[3] This does not mean that the board is straying, or should stray, into executive territory. Boards almost always reserve certain decision-making powers for themselves, and in making those decisions they are determining the acceptance or not of the related risks. Boards also engage in discussion about risks, both known and unknown, and their significance. It remains the role of management to act upon the advice and direction given by the board and to implement its decisions.

We found evidence that some non-executive directors of corporates need to spend more time, or a greater proportion of time, with the business **outside the boardroom** – visiting operations and talking to management and staff at all levels of the company. Because of the importance of the human factor in risk management, gaining assurance and information in this way is a necessary foundation for a non-executive's effectiveness. However, this does not translate into a universal need for non-executives to spend more time in total. It can often be compensated for by economising on less productive activities, and by the management trying harder to provide information that is user-friendly for non-executives.

This emphasis on non-executives getting out and about in the business is part of a larger point, which is that they have to **understand the business in all its aspects**. In some cases, the **mix of expertise on boards** could usefully be widened so that the non-executives collectively are equipped to challenge on all the major risk areas. This has a separate relevance to audit committees, in some of which the oversight of complex, wide-ranging and sometimes very technical risk matters is being done by a group which contains mostly, or even entirely, financial expertise. This somewhat limited committee composition could be seen as encouraged by the emphasis placed on recent and relevant financial expertise in the Combined Code. There is a case for revision to reflect the fact that most audit committees have risk oversight as a major part of their role, often now a more challenging part than oversight of financial reporting and audit.

The importance of understanding the business also has implications regarding director longevity. In many large, complex businesses, learning about them is a never-ending process and it can take some years before a non-executive is equipped to be very useful. In some cases, they become useful not long before being required to stand down on the supposed grounds that longevity creates a threat to independence. We have long been of the view that comply-or-explain needs to be made to work properly in relation to director independence and that **the so-called Nine Year Rule** should be clarified or, preferably, substantially amended. The evidence in this report adds weight to this view. (It should go without saying that, if that accumulated knowledge is to be useful, the personal qualities needed to challenge constructively and effectively must be maintained over the years.)

What of the 'well-they-would-say-that-wouldn't-they' problem? Since this report is based on evidence gathered largely from those responsible for risk governance in corporates, can it be more than a compendium of corporate complacency? We think it can. For one thing, we certainly didn't come away from all our interviews feeling impressed by the quality of risk governance that we'd just encountered. And we critically compared different points of view from within the same company, and the attitudes of separate categories of survey respondent.

But convincingly executed or not, the same underlying principles of risk governance appeared throughout, with quite remarkable consistency. And so the conclusion we draw is that **it's not the principles of risk governance which need attention, but the way in which companies turn them into practice**.

One of the ways that corporate boards can help to ensure that good principles get turned into good practice is by **taking a good hard look at themselves**, and a number of the chairmen that we interviewed spoke of the benefit of board evaluation in helping to improve its work. The Walker Review emphasises the need for a board to undertake rigorous evaluation of its performance, for reasons which are just as applicable to corporates.

Walker also recommends that external review should be used every two or three years, because the critical input given by a qualified external reviewer can be a catalyst for board awareness and improvement. It is difficult to see why corporates should be different, since directors of any sort of company are not exempt from the well-researched human tendency to exaggerate the degree of control we have over events. This is visible in our survey results – for example, audit committee chairmen are consistently rather more confident about the quality of assurance received by the board than are other respondents, and chairmen are consistently the most happy with the way that agenda time is used. This suggests that corporate boards, just like financial services ones, would benefit from periodic independent challenge to their self-perceptions.

And a final thought. We were impressed by the not inconsiderable number of companies on our interview list which had had the opportunity to learn about risk governance from experience. Putting it less diplomatically, some were still recovering from

disasters, or at any rate had relatively fresh memories of them. The big **lessons from past crises** were really very simple: that management had to do its job properly, structures and processes had to make management's job easier, and that the board had to be alert to what management were doing. None of these companies had found a magic wand to put things right; none had found the answer in any single reorganisation or process re-engineering. **Determined leadership and thoughtful judgements** by the CEO, executives and board were the critical factors.

Even after years of hard graft, these companies were still working at things. Getting it right isn't something that can be done quickly, and it won't ever be finished. But the evidence in this report gives some pretty clear pointers to what boards and management have to do to keep things going in the right direction.

This report describes some matters where we found evidence that things were not always working as well as they should. To help boards ask themselves whether these apply to them, they are identified like this: 

>>>

**In the course of this study we came across a lot of interesting ideas – things that worked well for somebody, if not for everybody. These are scattered around the report in little boxes just like this one.**

# SCOPE OF THIS REPORT

This report describes the findings of Independent Audit Limited's investigation of risk governance at large UK listed companies outside the financial services sector. It was undertaken in the context of recent difficulties at a number of financial services organisations, the consequent concern over the effectiveness of their risk governance, and the emergence of various proposals for structural reform aimed at improving it. The question therefore arose as to whether structural reforms are also required in non-financial services organisations. Independent Audit was engaged by The ICAEW Foundation to undertake a study 'to identify whether there is evidence supporting the need for changes to the Combined Code in relation to this issue'.

Two streams of work were undertaken as part of the study.[4] One consisted of interviews with directors and officers from 29 FTSE 350 companies. A total of 79 interviews were held. Interviewees were mostly chairmen, chief executives, finance directors, audit committee chairmen and heads of internal audit, plus a few chief risk officers ('CROs') and company secretaries.

The second stream consisted of questionnaire-based surveys of 131 people across 45 companies, including 15 companies which were also among those interviewed. Separate questionnaires surveyed the opinions of non-executives and 'management' (the latter group for this purpose including heads of internal audit, CROs and company secretaries). In addition to these opinion surveys, 58 company secretaries provided factual information about the organisation and practices in their companies.

The charts and statistical information given in this report all come from the various questionnaire-based surveys, with the interviews informing their interpretation. Each chart is separately identified as NED, management or factual.

The number of companies that participated in some way in this study totalled 59 out of 251 non-financial services companies in the FTSE 350,[5] or 24%.

4 Full details of the methodological approach are set out at www.independentaudit.com/publications and www.icaew.com/foundation

5 FTSE list as at the end of May 2009 and including one participant which was ranked 354.

# FINANCIAL SERVICES ORGANISATIONS VS CORPORATES

**'Financial institutions and non-financial institutions are very different in terms of risk.'**

Without exception, those we interviewed expressed the strong view that the differences between financial services organisations and corporates are so marked that conclusions regarding risk governance in the former should not be applied wholesale to the latter. This was argued with particular clarity and vigour by those who also had current or past experience of sitting on the boards of financial services organisations. Three main reasons for maintaining this distinction were frequently given: the nature of risk in relation to the business, the impact of risk on the balance sheet, and the importance of financial reward.

## THE NATURE OF RISK IN RELATION TO THE BUSINESS

**'Risk [management] is an inseparable part of good management.'**

Financial risk dominates the day-to-day business of a financial services organisation, where the stock-in-trade is money. Because of this, and because it can by its nature be expressed in numbers, financial risk management exists as a major control activity and is the foundation of financial services regulation. By contrast, the day-to-day business of a corporate is primarily concerned with 'operational risks', more broadly defined than in financial services, and which are much more difficult to measure in financial terms. Some risks, such as the risk of loss through contract overruns, can be estimated financially, but in many other cases (such as health and safety or the delivery of essential services to the public) the financial quantification of exposure and appetite is usually impracticable or unhelpful, or both.

In financial services organisations, risk is usually approached in separate categories such as credit risk and market risk, each being separately used in the calculation of the capital cushion required. Operational risk is one of these separate categories, covering a wide range of risks including those relating to people, process and organisation. It is usually the category which is the most difficult to calculate for capital purposes.

In corporates, risk is not used as the basis for calculations of required capital. Nor has it been broken apart in the way that it has in financial services organisations. Instead, what is usually known as operational risk reflects the full spectrum of management activities involved in running a business. Corporates treat the management of risk as an inseparable part of business, and therefore as an inseparable responsibility of line managers.[6] Risk managers are not widely used as a control function and the financial measurement of risk is restricted to specific cases where it is both practicable and useful, such as contracts and treasury activities.

## THE IMPACT OF RISK ON THE BALANCE SHEET

**'A financial services balance sheet can blow up overnight. It usually takes a lot longer in a corporate.'**

Not only do financial services organisations have very much bigger balance sheets than corporates, the financial risk contained within them is of a different order of magnitude. They are built up from a very large number of transactions, each of which contains some amount, often a large amount, of financial risk. The volume of transactions, not to mention their variety and complexity, means that in all but the smallest financial services organisations the board's contact with individual transactions will not relate to a significant proportion of the total risk exposure in the balance sheet – a risk exposure which, as has been vividly demonstrated in the last couple of years, can blow up at short notice.

In the absence of systematic fraud, the risks arising from a corporate's day-to-day activity are unlikely to accumulate unseen to the point of threatening the company's existence. With only occasional exceptions, poor management of the day-to-day business leads to reputational damage and/or poor financial performance, rather than to sudden death. This hardly provides grounds for complacency – poor management is always bad for shareholders and, sooner or later, for executive careers – but its gradual emergence means that there is time to react and for damage to be repaired before the company reaches the point of collapse or, more likely, being taken over.

6 In theory, this is how it should be in a financial services organisation as well. But in practice the breaking up of risk management into functional specialisms can often go against this.

A large part, often the largest, of the risk in a corporate's balance sheet arises from more strategic transactions that take place at a plc level: acquisitions, major investments, unusually large contracts, financial structuring. While these low-volume but high impact plc-level transactions represent a threat to financial services organisations and corporates alike, they are a relatively much more dominant factor in corporates' risk exposure. By their nature, these transactions are both relatively infrequent and much more readily visible from the boardroom than the day-to-day transactions which dominate a financial services balance sheet.

## THE IMPORTANCE OF FINANCIAL REWARD

**'Significant risks from incentives exist only at the executive level.'**

Financial incentives play a smaller part in corporates than in most financial services organisations.[7] We found that high-value performance-related incentive schemes are normally reserved for only a small number of senior executives, who are within the scope of the Remuneration Committee, and for sales staff, where the related risks are well understood. For the rest, performance-related pay is usually a relatively minor part of the total reward and is commonly influenced by the company's performance as much as or more than personal performance.

Consequently, the motivating power of financial incentives is not pervasive, and other, non-monetary, motivating factors can be at least as significant if not more so. In fact, several interviewees told us that where significant breaches of policy had occurred, it was as likely to have been in a misguided effort to benefit the company as for personal gain.[8]

## FINANCIAL SERVICES ACTIVITIES WITHIN CORPORATES

**'We're a non-regulated holding company with a regulated subsidiary which has its own non-executive directors.'**

Many non-financial services companies do of course have financial services-like activities within them (for example commodity trading in food processing companies, retail banks owned by supermarkets and treasury activities in every large company). These are clearly identified activities within their corporate parents and were described to us as having risk management and control arrangements that conformed to normal financial services practice. In some cases, particularly where the activity was conducted in a separate legal entity, they had their own governance arrangements.

In none of the companies interviewed were financial services activities so large as to mean that the company interviewed was actually a financial services organisation in disguise. Where financial services activities had their own separate governance arrangements within companies interviewed, we excluded these from the scope of discussions and in consequence this report does not address as a separate topic the governance of financial services-like activities within corporates.

Financial risks which are part of business-as-usual (for example, customer credit risk) are regarded by corporates as part of operational risk, and were therefore included within the scope of our discussions.

7 It is only fair to acknowledge that, despite headlines to the contrary, there are a lot of people working in financial services for quite unexceptionable incomes.

8 This was in the context of breaches at lower levels in the organisation. The danger of 'greed, hubris and the desire for power' remains as real in corporates as it does in financial services organisations (*Greed and Corporate Failure*, Hamilton and Micklethwait, 2007).

# RISK MANAGEMENT, RISK GOVERNANCE… WHAT EXACTLY ARE WE TALKING ABOUT?

**'The CEO is the CRO.'**

**'It's the day job.'**

**'[Managing] risk runs throughout the way we work.'**

Almost without exception, and for the reasons outlined above, none of those we interviewed considered risk management as something that could meaningfully be separated from business management. As a concept, risk management was understood to mean managers and staff (and where appropriate agents and subcontractors) understanding the risks around what they are doing and making well-judged decisions that reflect a consistently-understood attitude towards risks that the company will accept or encourage. As a process, it referred to the identification and reporting of risks to enable cost/benefit decisions about mitigation and assurance. To the extent that it exists at all as an organisational function, Risk Management was found as a small, group-level body of people whose job is to facilitate the identification, appreciation and reporting of risk by management.

**'Good risk management is part of good management.'**

Many of our interviewees were quite happy to talk about 'risk governance'. Others disliked the term, preferring 'risk management', 'risk oversight' or 'risk responsibility', although without necessarily meaning the same thing as others who favoured the same expressions. While each individual was clear enough about what it meant in terms of what they personally had to do, the lack of clarity in terminology was generally unhelpful and sometimes led to a lack of clarity in relation to organisational responsibilities.

All those we interviewed regarding a board's responsibility for risk were actually talking about two main things, and it will be helpful to maintain a clear distinction between them. Because operational risks are inseparable from other aspects of the business, risk management is something that takes place across the entire organisation, with risk reporting used as a tool to benefit management performance and accountability. Because of the volume and diversity of risks across the organisation, the role of the board in relation to this aspect of risk management is to exercise **oversight** of the management, including receiving **assurance** on the relevant processes.

The other category of risks is those which are individually significant at plc level, and are approved at board level. While these are mostly corporate matters such as M&A, financial structuring and threats to the achievement of strategic goals, operational risks can sometimes also be significant at this level, either because they arise from unusually large transactions, a major hit to reputation or because of something systemic across the business. At this level, the role of the board goes beyond oversight: the board is itself engaged in certain aspects of risk management. Those aspects can include the **identification, assessment and acceptance** of these significant risks. Continued monitoring of the risks and taking actions in mitigation, however, remain the responsibility of executive management.

This report will make the distinction between the two ideas by using the terms '**board oversight of risk processes**' and '**board-level risk acceptance**'.

While its work sometimes involves specific consideration of significant risks and uncertainties, it is equally true to say that almost everything the board does involves taking risk into account and making informed judgements. Whether agreeing strategy, setting remuneration policies or approving large transactions, the board will benefit from good information and well-organised processes, but these are likely to be specific to the matter in hand rather than being the same processes used in relation to operational risk.

In some cases, the lack of clarity in terminology had resulted in companies trying to use a single process to encompass both 'board oversight of risk processes' and 'board-level risk acceptance'. While directors nonetheless knew what needed to be accomplished, getting it done was sometimes not as straightforward as it might have been had there been greater clarity. Some companies might find it useful to reassess their practices in the light of this distinction.

# HOW RISK RESPONSIBILITY IS ORGANISED

**'Our biggest challenge is to keep the process alive.'**

We found considerable variety in the ways in which companies structure themselves in relation to risk. Underlying that variety, however, there was a consistent set of principles.

## THE BOARD'S RESPONSIBILITY

**'Risk is a board issue. It is hardwired into all board and executive debates.'**

Most interviewees believed that the whole board bore the responsibility for ensuring that the company did not take on excessive or unrecognised risk. This is what might be expected, in view of the requirements of law and the Combined Code. Where interviewees seemed to say otherwise, this generally reflected terminology issues.

However, a significant number of interviewees expressed a more generalised concern regarding the growing expectations of non-executive directors (NEDs). Political and media comment appeared to take it for granted that NEDs should prevent a company from ever getting into trouble. All felt strongly that this was not only wholly unrealistic, but also undesirable – if risks are taken, then despite even the very best efforts things will sometimes go wrong. The only way NEDs could try to prevent anything going wrong would be to prohibit risk-taking, which would not be in shareholders' interests. NEDs did not join boards in order to become Business Prevention Officers and were concerned about the public expectation of their role appearing to drift in this direction. In addition, the very fact of being non-executive meant that NEDs had limited information and necessarily had to trust the executives. As described further below, this meant that a key part of the NED role was determining whether that trust was justified, but no-one could guarantee 100% success in a matter so dependent on subjective judgement.

In a small handful of cases, however, interviewees went beyond these reasonable concerns about the limitations of NEDs and expressed a much more negative view – that the practical constraints on NED effectiveness meant they couldn't be expected to achieve very much. If this were true it would leave NEDs in a rather invidious position, since in law they carry equal responsibility with executive directors. It is more likely that a realistic and reasonable expectation of NED contribution lies somewhere between these extremes of too high and too low. Shaping public perceptions may be beyond any one company's influence, but individual boards could usefully spend time ensuring that at least their own directors are on reasonably common ground regarding what can be expected of them.

## BOARD COMMITTEES

**'We discussed it but didn't think there was any need to have a separate risk committee as the board is fully engaged on managing risk.'**

There was almost no support for regulation to mandate a separate risk committee of the board. Only one interviewee felt that a separate committee was needed, and that for specific reasons dealt with separately below. A handful of interviewees were neutral and the majority were firmly against it. A number of companies had considered creating one, but there was a very strong feeling that it was not merely unnecessary but could be positively unhelpful. Because risk management is inseparable from good management of the business, it should not be divorced from the other work that the board does to hold management accountable, and there were real concerns that the creation of a separate risk committee could lead to those who are not members of it disengaging from responsibilities that are fundamental to the board as a whole.

There is however a role for the audit committee. For companies that are subject to NYSE requirements, the audit committee must 'discuss policies with respect to risk assessment and risk management'; and while the Combined Code is on the face of it more flexible, the fact that it requires the audit committee to oversee internal audit means that the audit committee will always be involved in at least some aspects of risk management. More than half of the companies surveyed give the responsibility for 'board oversight of risk processes' to the audit committee, with the responsibility in most other cases belonging to the board. See Figs. 1–4

Fig. 1 (Factual questionnaire)

**Which part of the board structure is responsible for doing the work necessary to recommend board approval of the Combined Code ('Turnbull') statement on internal control?**

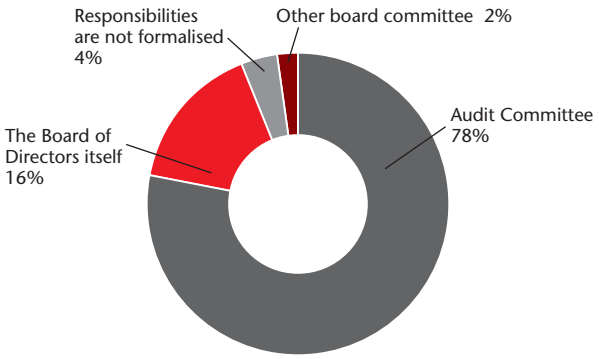



Fig. 2 (Factual questionnaire)

**Which part of the board structure is responsible for making sure the business has sufficient risk management capability/competency?**

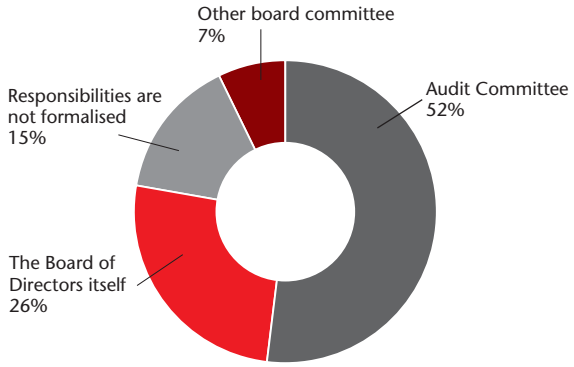



Fig. 3 (Factual questionnaire)

**Which part of the board structure is responsible for assessing the effectiveness of the risk identification process?**

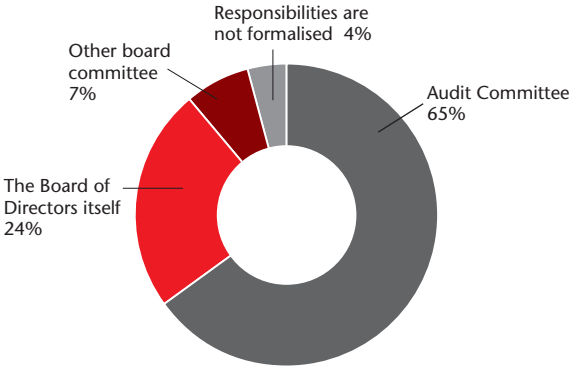



Fig. 4 (Factual questionnaire)

**Which part of the board structure is responsible for reviewing the alignment of the risk profiles used by different parts of the assurance framework?**

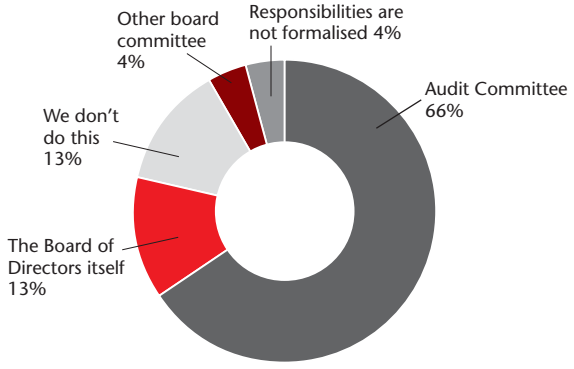
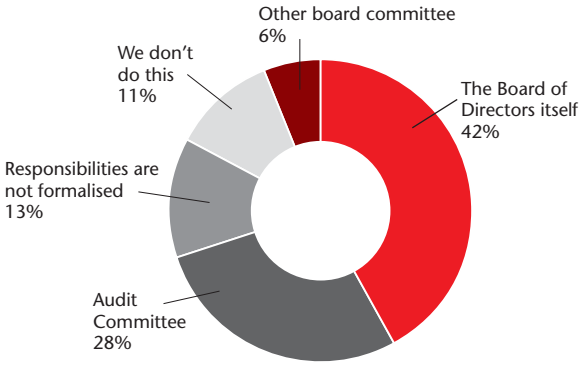


Fig. 5 (Factual questionnaire)
**Which part of the board structure is responsible for developing, for the board's review, the statement of risk appetite/risk tolerance?**




This frequent location of oversight responsibility no doubt contributes to the fact that, among NED respondents to our survey, audit committee chairmen were the most confident of the visibility and oversight of risks.

Interviews revealed a similar pattern regarding location of responsibilities. The most common arrangement was that the audit committee was responsible for oversight of the risk processes, while the board was responsible for 'content', by which was meant 'board-level risk acceptance' – taking strategic or highly material risk decisions and assessing the major risk positions that result from taking risks and mitigating them. A substantial minority said that the whole responsibility for oversight and risk acceptance lay with the board.

Most interestingly, a further substantial minority said that the whole responsibility was with the audit committee. This last point is confirmed by the survey which shows that a quarter of companies give their audit committees the responsibility for developing the statement of risk appetite, an indicator of 'board-level risk acceptance'. See Fig. 5

On the face of it, giving wider responsibility to the audit committee (ie, including 'board-level risk acceptance' as well as 'board oversight of risk processes') appears to be in conflict with the almost universal view that risk is the responsibility of the whole board. We found, however, that appearances are not what they seem. In many of the companies interviewed where the audit committee was said to have primary responsibility for risk, all NEDs and all or most executive directors attend the audit committee meetings for either the whole meeting or for that part which deals with risk. So it is to all intents and purposes the whole board, using the audit committee as a convenient way of structuring its workload[9]. In most other cases where the audit committee was said to have primary responsibility, it was clear that there was substantial overlap with the board's work and little evidence of delegation to the audit committee in practice.

However, a few companies did give wide responsibility for risk to their audit committee and relied on reporting to the board for keeping the other directors involved. This seems less persuasive than having all directors involved in the discussions.

In one case a chairman felt very strongly that a separate board risk committee is needed to ensure that sufficient time is spent on non-financial risks, given the other demands on audit committees and their natural bent towards financial reporting. These concerns were not shared by other interviewees. It was felt that the time burden could be managed and that the benefits of keeping all risk and control matters under the oversight of a single committee, thus avoiding the danger of matters falling down the cracks, outweighed the disadvantages of increased workload.

>>>

**Split the audit committee agenda into two – financial reporting and risk. Better focus, and easier to involve different groups of directors and management.**

9 While this might be convenient for risk oversight, if not carefully managed it has the potential to hinder the Audit Committee in its work on financial reporting and audit. In this context, splitting the agenda seems a particularly good idea.

However, this unease about the idea of a mandatory board committee for risk does not mean that it cannot be useful on occasion. While it need not be mandated, nor need it be outlawed. Some companies happily had a separate board committee for a particular class or classes of non-financial risk which needed an especially high level of attention. The most common was a Corporate Social Responsibility Committee, or something similar under another name, playing a role in overseeing, for example, risks relating to the environment or the employment of child labour. In some cases, this remained secondary to the audit committee and reported to it, so becoming one of the things over which the audit committee had oversight. In other cases, there was a formal division of oversight responsibilities, with a structured basis for coordination and internal audit reporting to both committees.

Despite the varying distribution of formal responsibilities, even despite sometimes unclear labelling, NEDs are very confident that they have a clear picture of what needs to be done by whom.

See Figs. 6 and 7

It therefore seems clear that the formal structure of board committees need not be a matter of the greatest significance. What matters most is that, in one place or another, all directors are involved in 'board-level risk acceptance'. Delegating 'board oversight of risk processes' to the audit committee is widespread practice and appears to work well, particularly if the audit committee possesses relevant business expertise as well as financial skills and experience. This last point is considered more fully later in this report.

Fig. 6 (NED questionnaire)

**The responsibility of the board and its committees for oversight of risk management effectiveness is well understood.**

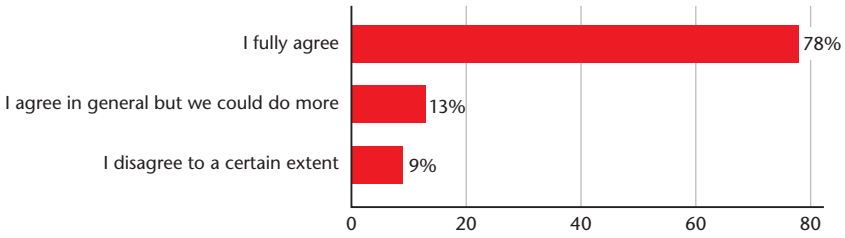
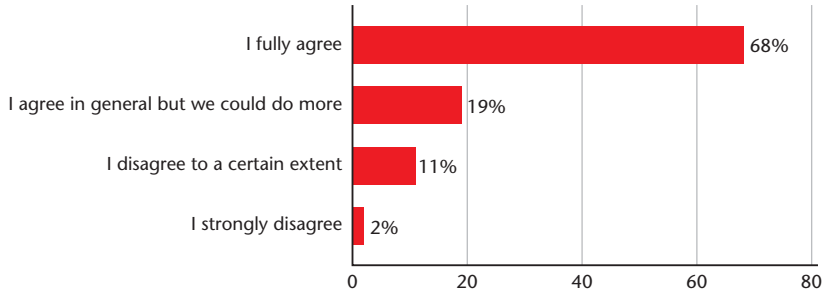



Fig. 7 (NED questionnaire)

**The split of responsibilities for risk management oversight between the board and the board committees – and between each of the committees – is clear.**



One company interviewed had the practice of forming a special sub-committee of NEDs to play devil's advocate in relation to proposed acquisitions. Others dealt with it in the main board. The devil's advocate idea seems a good one, in view of the known perils attached to acquisitions, which other companies might benefit from adopting. The essential element is the role to be played by nominated NEDs, rather than the existence or otherwise of a sub-committee, and it is not obvious that mandating the formation of such a committee would be helpful.

>>>

**For large, high-risk transactions, ask a NED or two to play devil's advocate.**

## MANAGEMENT COMMITTEES

**'We have a risk committee – it is an executive committee with NED representation.'**

Many companies have one or more management committees, sometimes a group-wide hierarchy of management committees, with explicit responsibility for risk management. These are found to be a useful part of the risk management process, both as a means of obtaining managers' input and also for reinforcing the importance of risk management throughout the organisation.

It is however important not to confuse these management committees with board committees. If a company has something called simply a Risk Committee, it is almost always a management committee and not a board committee. This applies even if, as is sometimes the case, one or more NEDs are members or regular attenders.

# THE HUMAN FACTOR

**'The most important thing for a business is to have intelligent and honest people.'**

**'Good managers are good at risk management.'**

**'[The company had been] too rule-bound… it needed to move to a principles- and values-based culture.'**

The most strikingly consistent theme to emerge from our interviews was that, since risk management is inseparable from good management, it is all about people and culture. We were initially surprised by the number of hard-nosed businessmen and women who very quickly took the discussion to topics such as culture, values and leadership; but the surprise wore off quickly, and by the end of our work the few who did not emphasise these matters stood out as exceptions.

**'CEO leadership and tone at the top are critical.'**

**While practices varied, certain key principles were widespread.**

## Leadership

The CEO and other senior executives must be visibly committed to demonstrating the values that underpin the behaviour expected across the organisation. They must invest time and enthusiasm in being seen to support internal audit and good risk management practice. While some were initially sceptical of new initiatives to strengthen risk identification and reporting, they were soon converted, primarily by a recognition that stronger risk practices meant for better management. Efforts made by internal audit or CROs to avoid risk becoming a parallel process and to keep it fresh also encouraged CEOs to give support.

The role of the chairman in providing leadership to the board and to the CEO is also critical.

## Tone at the top

The board must send consistent messages on values and behaviour, and the chairman and NEDs, particularly the audit committee chairman, should seize opportunities to reinforce these.

## Openness

Companies need cultures that permit, indeed encourage, people to own up when things are going wrong, so that action can be taken and lessons learnt.

**'A trigger is responding to failures. The experience of examining what went wrong enables [management] to identify ways of improving the process.'**

## Firmness

The most shocking failures, above all those of concealment, must be dealt with uncompromisingly. 'Public hangings' can be used to send a clear message regarding the importance of core values, but not for poor performance.

**However, the emphasis on people does not mean that process and structure do not have their place. Once again, certain key themes emerged.**

## Accountability

It is essential that people know what they are responsible for, and to know that they will be held to account for how they use their authority. This means, among other things, clarity of risk ownership; having clear reporting lines and authority limits; good information systems; and effective internal audit.

## Process

Certain processes reinforce accountability. These include self-certification and sign-off (with audit); and even the dreaded Sarbanes-Oxley, which, now that the documentation and audit components have been reined in, has settled down to something that many of our interviewees thought was useful. The benefits described to us included the establishment of clear process, ownership and accountability.

## Policies

The board's expectations on critical matters need to be clear, which usually means they need to be written down (and then made accessible to all who need to know them). So far as possible they need to be consistent across the entire organisation.

## Engagement

Tone at the top is valueless if it does not extend beyond the boardroom doors, and companies need to make practical arrangements to ensure that the NEDs have enough engagement with managers below executive level.

## Learning from failures

Losses and near misses are among the most important sources of information on risk management that any company can have – but the learning will not happen unless it is managed.

## Risk reporting

While practices vary, having some formal process of risk identification and reporting helps to focus attention and to inform cost/benefit decisions on risk mitigation. Some degree of formality, at least enough to make management activity visible, is also necessary if NEDs are to be able to exercise oversight of the risk processes.

A few interviewees observed that ownership of shares by employees made them more risk-aware.

>>>

**Build learning from mistakes – and successes – into the management processes.**

**Give clear mandates with words like 'line leaders shall…'**

# THE ROLE OF THE BOARD AND NON-EXECUTIVE DIRECTORS

**'The management mindset must be that risks must never be concealed. This needs to be set by the tone from the top.'**

**'The board's primary job is to create a culture and communicate an appetite for risk – if not done deliberately, it will be done by default.'**

## KNOW THYSELF

**'Board effectiveness reviews, both external and by self-assessment, help to improve risk over sight.'**

The role of the board in relation to risk was the primary object of this study, and those interviewed were mostly executive and non-executive directors, together with heads of internal audit and a handful of CROs and company secretaries. Hardly surprisingly, almost all those interviewed thought that the board was very important to a company's management of risk.

Rather more alarming was the very small number of companies whose executives thought that their board did not make much of a contribution – especially since non-executives from the same companies took a different view of the matter.

These may be extreme examples of something shown by our survey, which indicates that CEOs are somewhat less positive about the role of the board than are other respondents, while chairmen and audit committee chairmen are generally rather more positive about the matters for which they have responsibility than are others.

This should not be surprising. It is a normal human tendency:

> Most people are highly optimistic most of the time. Research into human cognition has traced this over-optimism to many sources. One of the most powerful is the tendency of individuals to exaggerate their own talents – to believe they are above average in their endowment of positive traits and abilities… We also tend to exaggerate the degree of control we have over events, discounting the role of luck.
>
> (*Delusions of Success*, Harvard Business Review, July 2003)

It is difficult to draw too many conclusions from this. However, it does perhaps support the view expressed by a good number of interviewees, that formal reviews of board effectiveness are valuable in strengthening the board's work, including that on risk. As some NEDs pointed out in relation to their own work, the most effective counter to over-optimism is good constructive challenge. It is difficult to see any reason why the same principle should not apply to the board itself. The Walker Review's recommendations regarding board performance evaluation and reporting (Recommendations 12 and 13) would therefore appear to be generally applicable, not merely to financial services organisations. It might however be preferable to avoid the term 'evaluation', which seems to have led some directors to view it as an annual pass-or-fail exercise (and therefore prone to a box-ticking approach) rather than as an opportunity for self-improvement.

A further discrepancy arose in relation to satisfaction with the present state of risk management activity. NEDs surveyed were very positive that management was doing as much as could reasonably be expected to manage risks. See Fig. 8

However, questions aimed at eliciting executives' 'wish lists' showed strongly that they would like to do more to make sure that risk management was working well and was consistent across the business.
See Figs. 9 and 10

Fig. 8 (NED questionnaire)

**Management teams do as much as can reasonably be expected in identifying risks and implementing an adequate response.**

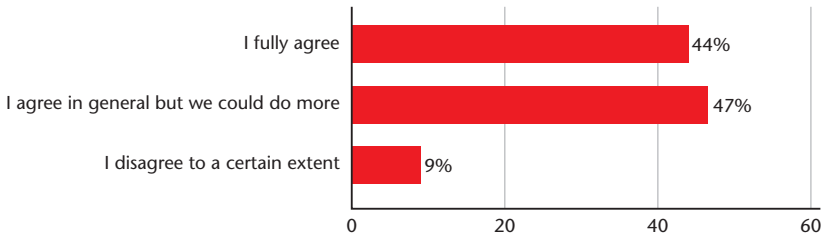



Fig. 9 (Management questionnaire)

**If I had more resources, I would invest more in spending more senior management time on making sure that risk management processes and controls are working well.**

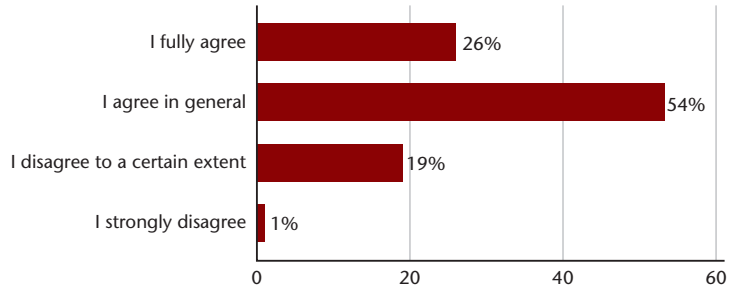
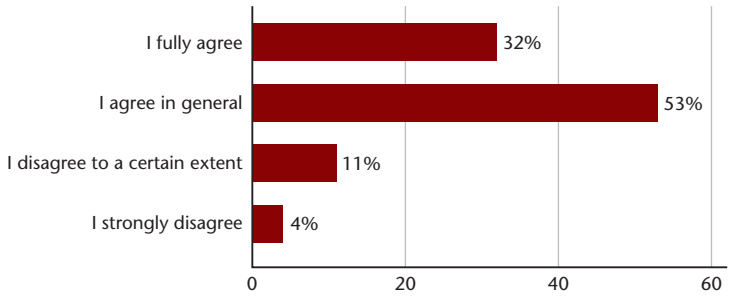



Fig. 10 (Management questionnaire)

**If I had more resources, I would invest more in ensuring that the quality of risk management is consistent across the business**



For each company where we had both management and NED survey respondents,[10] we compared their answers to similar questions. Answers to questions relating to the board itself showed only random differences. But answers relating to the effectiveness of risk management within the organisation gave a different story.

The table below shows the three questions that gave rise to the greatest divergence of view. On a five point scale, where 1 is the lowest and 5 the highest degree of comfort, the average comfort of NEDs exceeded that of management by sizeable margins. In addition, for these three questions, the difference in view was systematic: lower scores were given by management in almost every separate company.

In short, the survey did not find a significant difference of opinion between NEDs and management regarding the board itself. But it does suggest that NEDs have a systematic tendency to be more at ease with the risk management than do the executives responsible for running it.

We put this down to a combination of factors. One is that most things look better from a distance, and NEDs are relatively remote from the practicalities of most risk management activity. This reinforces the need for NEDs to guard against over-optimism and the ever-present threat of complacency.

The other, offsetting, explanation is that most executives do take risk management very seriously, as we saw in our interviews; they know they could always do more and so are readier to acknowledge that in an ideal world they would spend more.[11]

We would not want to overstate the significance of these issues. The statistical evidence is of a general but modest tendency and does no more than illustrate what ought to be expected given that even those engaged in risk governance are human. Encouragingly, almost all of our interviews showed that executives and non-executives were facing the same way. Even if there were varying degrees of caution over how well it was working in practice, there was a high degree of consistency over what was necessary for a board to be effective in its governance of risk. The key elements are described in the following sections.

Table 1
**How well...**

| | Management average score | NED average score | Difference in average scores | Companies where management scored lower | Companies where NEDs scored lower | Companies where NEDs and management scored the same |
|---|---|---|---|---|---|---|
| **Is risk management embedded?** | 2.1 | 4.2 | 2.1 | 23 | 0 | 1 |
| **Does risk management keep up with change?** | 2.3 | 4.1 | 1.8 | 24 | 0 | 1 |
| **Do risks find their way up the organisation?** | 2.7 | 3.8 | 1.1 | 16 | 5 | 4 |

10 Between 24 and 27 companies, the number varying for each question because not all respondents answered every question.

11 This explanation is given additional credence by the fact that within the management group, CFOs and heads of audit gave consistently lower scores than CEOs – exactly what one would hope to be the attitude of a good CFO or auditor.

## THE CHAIRMAN

**'The way the chairman runs the board is crucial.'**

**'An independent chairman – ie, not a previous executive – is critical. You need someone who has a powerful controlling influence over the CEO.'**

**'The chairman must encourage in-depth debate by the NEDs and… ensure that NEDs challenge executives sufficiently over matters that they do not understand.'**

A number of interviewees specifically mentioned the importance of the chairman role, and in other interviews it was frequently implicit.

The chairman is critical in relation to board composition, which as described below is a key component of effectiveness in relation to risk governance.

Also most importantly, the chairman plays a key role in creating an environment in which executives are receptive to challenge and in which NEDs give it constructively. In particular, the chairman can influence the attitude of the CEO to the board in a way that will enable the board to be more effective.

## THE CEO

**'You need a CEO (and a CFO) who is prepared to take counsel.'**

**'The CEO focuses on values and culture change… it is critical that the CEO believes in it and lives it.'**

As already noted, the role of the CEO in leadership of the organisation is critical to good risk management. If this is not well done, the principal contribution of the board, and most importantly of the chairman, is to encourage it, and in an extreme situation to replace the CEO. Replacing a CEO is not something done lightly, and is particularly difficult without some sort of crisis to provoke it. Consequently, a number of interviewees mentioned the importance of the CEO's receptiveness to challenge.

As well as his or her personal willingness to take counsel and benefit from challenge, the CEO also needs to value the processes and information that are necessary to enable NEDs to provide effective challenge. This is particularly relevant in organisations which have a very hands-on management style – often very effective, but which can be difficult for NEDs to observe and assess. Some degree of formal reporting is usually necessary for effective oversight, and for the board's sake the CEO needs to be committed to the relevant processes, even if they do not seem to give much direct value to executives who are deeply involved in the business.

In relation to 'board-level risk acceptance', some interviewees also noted the importance of not being presented with completed proposals when it was too late to have significant input and which could only be rejected at the risk of a major confrontation with the executives. Avoiding this means bringing proposals to the board while they are not fully formed, which in turn requires the NEDs to refrain from criticising proposals because they are half-baked. A few also mentioned the desirability of obtaining more independent advice on proposals, although it did not appear that this idea often went beyond being an idea.

>>>

**Arrange board approval processes to give room for more than a 'yes or no' decision.**

It was also clear from many of the interviews, particularly but not only those with heads of internal audit, that the CEO's visible support for internal audit is critical to audit's own effectiveness. In view of the widespread importance attached to internal audit, this must be another key element of the board's dependency on the CEO.

## OTHER EXECUTIVE DIRECTORS

**'It must be the person responsible who reports and presents the report to the board.'**

Most often, the CFO and other executives were bracketed together with the CEO as critical to providing consistent leadership across the organisation.

A number of NEDs emphasised the importance of having other executive voices around the boardroom table, and in particular the importance of an independent-minded CFO. However, a few took the

view that it was unrealistic to expect executives to risk undermining the CEO during board meetings, and that it was more important to have a strong executive committee at which executives could debate among themselves before bringing matters to the board.

Perhaps as a means of reconciling these opposing views, there was a widespread view that NEDs must have plenty of opportunities to meet executives, including those below board level, in circumstances other than formal board meetings – at dinners, site visits and management conferences, for example.

## NON-EXECUTIVE DIRECTORS

**'Management does need someone to look over their shoulder and make sure that [risk management] is happening.'**

Almost all interviewees felt that boards, usually through their audit committees, met their oversight responsibilities well. The discipline provided by 'board oversight of risk processes' usually had a positive effect on the quality of the management processes.

**'The board should provide content as well as impose discipline.'**

With the exception of those few, already mentioned, whose expectations of NEDs were low, all interviewees thought it important that NEDs should add value by contributing more than the discipline of oversight. Views differed regarding the extent to which this was actually being done. Most executives interviewed were complimentary of the contribution of their NEDs but a minority wished for more (contribution, not NEDs). Consistent with the survey results already given, a rather larger proportion of NEDs said in interviews that they added value through their contribution of content as well as by providing oversight.

Whether interviewees believed there was already a value-adding contribution, or had it on their wish lists, there was widespread agreement regarding what is needed if NEDs are indeed to add value to risk governance.

### Engagement

**'[Visiting business operations] is an invaluable process for the NED to understand and assess very quickly whether or not risk and control processes are working.'**

**'NED engagement with the company is very important for them giving value – so our engagement programme encourages them to make visits without red carpet treatment.'**

**'The hardest thing for NEDs is to understand the nuances of the business. They have to see the wood for the trees, but they can't understand what they are seeing unless they are also familiar with the trees.'**

**'They do not second guess management, but need to spend a lot of time in the business to get to know it.'**

By a wide margin, this came top of the list of what it takes for a NED to be able to add value. A large proportion of companies actively encouraged, or even required, NEDs to get out and about in the business, not only on formal occasions such as board visits to locations but also on informal visits, preferably unaccompanied by executives.

As well as being of direct benefit to the NEDs and enabling a more informed contribution, many believed that such visits are of real value to the company in that they help to disseminate the tone from the top and make local managers more aware of their accountability to the board. Many also observed that board visits to locations were invaluable occasions for helping the directors to get to know one another, and that this was important to the board's effectiveness.

In a significant number of cases, executives identified this as a key thing that they wanted to change: they want more value from their NEDs, and the NEDs spending more time in the business is an essential basis. Even in today's difficult financial circumstances, very few CEOs or CFOs regarded this as something to be economised on.

While there can be tricky practical considerations for far-flung groups, particularly those with major operations in remote or inhospitable locations, this would appear to be something that all companies must take care to sustain and where many NEDs could do more.

>>>

**Getting out into the business should include talking to receptionists, drivers and the shop floor.**

**Ask NEDs to mentor up-and-coming executives. It's good for the executives and also for the NEDs.**

**The audit committee chairman doesn't have to be the only one to meet the head of internal audit informally.**

Many interviewees pointed out that it can take many years before a NED really understands the business, particularly the more complex ones, and that requiring NEDs to stand down after six or nine years often meant losing them just as they were starting to be useful. While the Combined Code does not actually require this, it has been widely interpreted in this way. It might be useful to have clarification by the FRC of what lies behind the independence principles set out in the Code, with a view to discouraging investors and others from taking too simplistic a view.

### Character

**'NEDs have to have the confidence to speak up and challenge and disagree.'**

NEDs need to have the personal qualities that will enable them to stand their ground, but also to know when to yield. Being judicious as to where they make their challenge will ensure they draw the right attention to the things that really matter. They have to be independently-minded but also willing to listen and learn, and not be overly influenced by prevailing fashions. Perhaps most importantly, they need to be willing to risk looking foolish, and to ask the (possibly naïve) question that no-one else is asking.

### Expertise

**'A wide variety of skill sets means that NEDs have the expertise to challenge the execs.'**

Diversity was valued, but not for its own sake: it needs to be centred around what is significant to the company. Most executives and a large proportion of NEDs interviewed thought it important that the board should contain a cross-section of expertise, so that there was at least one NED with practical knowledge of each of the major risk areas specific to the company.

This also applies to the audit committee (and in the view of a few, to all committees). If the audit committee is to exercise the most effective oversight of risk processes, then it needs members who understand 'content' as well as process. Some companies have achieved this by including one or more NEDs with technical rather than financial expertise on the audit committee, while others address it by having the whole board at the committee meeting.

However, some boards had significant gaps in the range of expertise around the table, and/or audit committees consisting largely if not entirely of people with 'recent and relevant financial expertise' rather than industry or other relevant technical knowledge.

Increasing the industry knowledge on boards can bring problems of conflict, but many companies have been able to get around this. There are opportunities for others to review their board and audit committee composition in this light.

A number of interviewees mentioned the importance of training and continuous updating of NEDs' knowledge. Several also observed that in practice not a great deal of board training seemed to go on, while one noted that the NEDs who most need training are usually the most reluctant.

### Experience

**'Portfolio NEDs bring experience of multiple ways of doing things.'**

**'You need grey hair and experience – and to have been through a downturn.'**

A number of chairmen and executives expressed a preference for currently serving CEOs as NEDs. Since no company would want a NED who is a current executive of a competitor, this limits the relevance of their expertise. Presumably the answer is to strike a balance between currently serving executives and portfolio NEDs, who not only bring wider experience

but may also have had directly relevant industry experience in a previous executive role.

A few also pointed out the value that comes from NEDs who have been around long enough to have seen it all before.

Very few of those interviewed, whether NEDs or executives, believed that NEDs need to spend more **time** to be effective in their risk responsibilities, except in relation to getting out and about in the business. Rather, the time must be well spent, which puts a premium on both focus and efficiency.

Only one executive acknowledged the executives' own responsibility for helping NEDs to be efficient by providing them with papers and presentations that are of maximum usefulness and user-friendliness. A larger number of NEDs raised the issue.

One of the companies which placed the most emphasis on NEDs' active engagement in the business also had the fewest board meetings, and viewed this as an explicit trade-off that benefited everyone.

## SOURCES OF COMFORT

**'The quality of management and the trust you have in them is the critical factor… you need to see the whites of their eyes.'**

A substantial number of NEDs interviewed raised the question of trust in the management. Regardless of how hard they might try, restrictions on time and information mean that NEDs will always be in the position of having to trust the management. However, most followed this with the conclusion that therefore the most important thing for any NED is to ensure that this trust is well-grounded rather than blind trust.

There was widespread agreement that **internal audit** was a critical source of comfort, for NEDs and executives alike.

Along with internal audit, the most important source of comfort to NEDs in this regard (and indeed for executives, in relation to their own dependence on subsidiary management) was **talking to a wide range of management** – not just the group executives with whom they were regularly in contact, but managers at all levels and in multiple locations. This gives them sources of information which are independent of the executive. Even more importantly, in many eyes, it enables them to assess the company's culture – how values are understood and applied in practice.[12]

This is another major reason for the emphasis, already described, on NEDs' engagement with the business – without it, the quality of their assurance will be limited. And it is not only the getting out and about – many mentioned the importance of bringing lower-level executives to present at board and audit committee meetings.

Another aspect of this is looking for **evidence of discipline** – for example, in period-end reporting, in the physical tidiness of factories and warehouses, in health and safety.

**'A safe site is a profitable site.'**

Most also took assurance from the quality of the **risk reports** and the debate around them. Although there was a recognition of the danger that board risk reports may be overly summarised or focused on too few risks, there was general satisfaction with both the quality and scope of the reports, and the processes in place for reducing the picture presented to the board down to the key risks. The potential problem of 'over simplification' is being addressed by focusing on changes in risks, getting comfort over the quality of the 'narrowing down' process, and having trust in management's judgement. There may also be scope for removing some more operational risks from risk maps by thinking through the distinction between 'board oversight of risk processes' and 'board-level risk acceptance' as previously discussed.

Among those who expressed a view on external audit as a source of comfort on risk management, opinions were divided more or less equally between those who thought they were and those who thought they weren't. What is most interesting about this is the fact that there were some cases where the auditors were appreciated as a significant source of comfort, which shows it can be done. It might be possible for more companies to derive better value from the audit if they adapt the way they engage with their auditors, which should encourage open and constructive discussions between audit committees and their external auditors

12 Interviewees noted that NEDs of international companies also have to understand the local cultures to which it has to adapt. This brings with it the danger of being disproportionately influenced by the views of those local managers who are the most fluent speakers of English.

about what can realistically be expected and delivered. It would of course be necessary to recognise the possibility that extending scope beyond what is required for statutory audit purposes could increase the auditors' exposure to liability, and manage it accordingly.

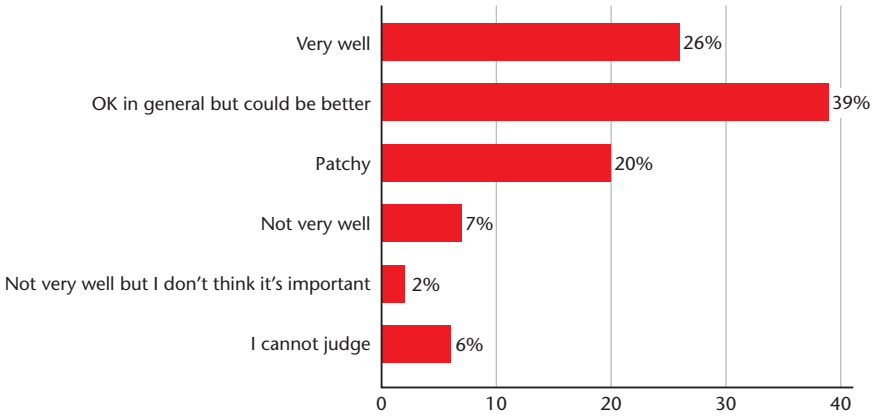
Some placed emphasis on being able to compare (sometimes called 'triangulating') information and assurance from multiple sources such as external audit, internal audit, management and, if there was one, the CRO. The inclusion of external audit on this list was offered as a reason for not wanting external and internal audit services to be received from the same provider.

Some interviewees mentioned **staff attitude surveys and reports on training programmes** as sources of comfort. Considering the importance that many people attached to culture and values, we might have expected more of them to mention such things. Few boards appear to have a clear view on how they might go beyond 'the smell test' on site visits to gain wider-reaching assurance on the risk culture (or corporate culture and ethical attitudes in general), despite a widespread recognition of its importance as a source of comfort. This looks like an area needing greater board attention and more practical steps to help the board form a view on the depth and consistency of attitudes and ethics.

The need for this is reinforced by the survey finding that over a quarter of NEDs expressed some degree of concern over how well they understood the picture of risk as seen lower down the organisation. Of all the questions about NEDs' confidence in the risk management processes, this one had the highest proportion of discomfort. See Fig. 11

Very few people included **whistleblowing** systems in the list of things on which they relied for comfort. Several of those who did mention it also remarked that it tended to be dominated by HR issues.

Fig. 11 (NED questionnaire)
**As a board we are good at getting the picture of how far there is alignment between the risks presented by senior management and those identified lower down the organisation.**



# RISK STRUCTURES AND PROCESSES

**'The formal process is a useful tool but it is not an end in itself.'**

**'Risk reporting is one of the best possible descriptions of the business.'**

**'Risks have to be actively debated based on the substantive rather than how pretty the forms are. Embedding requires executives and the CEO to lead by example.'**

## RISK MANAGEMENT AS A FUNCTION

**'To make people keen on this, keep it useful and simple. And don't let it sound like Risk Management!'**

Consistent with the belief that risk management is inseparable from good business management, none of the companies interviewed or surveyed had large Risk Management functions within their organisations. Where a separate risk management function exists at all, the most common arrangement is for there to be a head office team of less than five people with group-wide responsibility. From interviews, it was clear that their role was to facilitate the identification, appreciation and reporting of risk by management. See Fig. 12

A substantial proportion of companies does not have a formally constituted risk management function at all. Of those surveyed, 70% had a group risk function but the remaining 30% did not, and only 14% had separate risk functions in subsidiaries. See Fig. 13

Of those companies that did have risk functions, more than half – 54% – had risk management as part of internal audit.

The status of the Chief Risk Officer, or other officer fulfilling that role, varies widely. In about a quarter of companies surveyed, the CRO is a member of the Executive Committee, and in about the same proportion the CRO is a regular attender. This must be due to the fact that, as found by our interviews, CRO responsibility usually belongs to a senior business executive or to the company secretary, rather than it being a separate role. The other half of the companies surveyed are split evenly between having a CRO who is not of Executive Committee status, and not having a CRO at all.

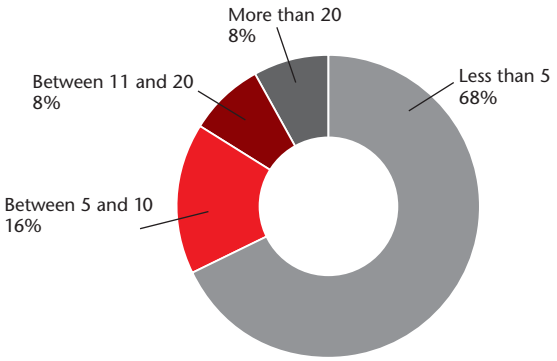



Fig. 12 (Factual questionnaire)
**What is the total headcount of the consolidated risk management function ie across the group (excluding internal audit)?**

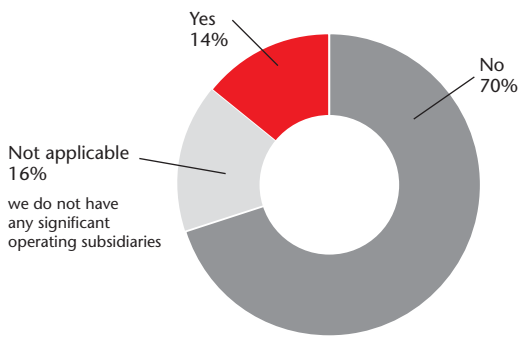



Fig. 13 (Factual questionnaire)
**Do you have separate risk management departments in the principal subsidiary companies?**

Fig. 14 (NED questionnaire)
**Generally Chief Risk Officers (or equivalents) should be members of company boards.**

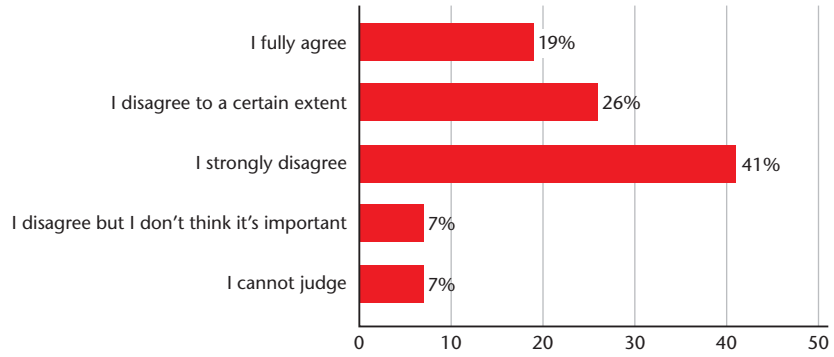
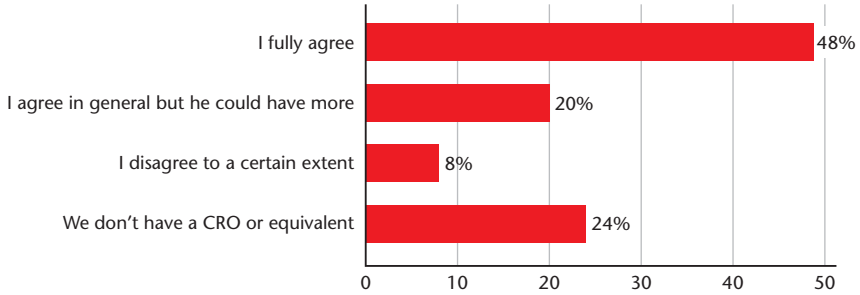



Fig. 15 (NED questionnaire)
**The Chief Risk Officer (or equivalent) carries enough weight in the organisation and is closely involved in management decision-making.**




There is no demand for establishing a separate CRO role at or near board level: most NEDs thought that CROs or their equivalents carried enough weight in their organisations, and less than a quarter of those NEDs who had an opinion thought that CROs should be members of boards. See Figs. 14 and 15

## INTERNAL AUDIT

**'Internal audit is the main assurance provider.'**

Internal audit came out well from this study. It consistently featured as one of the most important elements in a company's risk management. Slightly more often than not, as already noted, internal audit is formally responsible for facilitating the risk identification, assessment and reporting processes (a role that revolves around organising, with business management clearly responsible for 'ownership' of the risks).

Risk-based internal auditing is now the norm, with alignment between the risk basis of Internal Audit's work and the overall risk register and profile a key element of audit effectiveness. This means that internal audit has to undertake risk assessment work anyway. Combining this with facilitation of management's risk identification processes means that internal audit is playing a right-first-time role which is of more value to the company than waiting to see what management has missed.

There were mixed views on whether this combination of roles represented a threat to internal audit's independence. For some, this was a primary reason for having quite separate departments. In other cases, a separate risk management group had been established within internal audit, reporting to the head of audit but otherwise distinct. In these cases, heads of audit were aware that they should not be auditing their own department's work and that they should obtain periodic independent assurance on the risk management activity.

However, many held that the advantages of integration outweigh any potential threat to independence, and that this danger is mitigated by making it clear that 'ownership' of risk lies with management and that internal audit's role in risk management is facilitation only.

Many internal audit functions were responsible for providing assurance on a wide range of matters, reaching into operational activities as well as financial. Only a handful had a purely financial scope.

A number of companies had significantly strengthened their internal audit departments over the last few years. Despite the financial pressures that companies are under, none of the heads of audit interviewed reported that they were under pressure to reduce their resources. The survey indicated that both management and internal auditors felt that what was needed was not additional resources but rather more focus on embedding and improving the quality of risk management. **'It is not about more resources – the major risk areas require time to debate and consider the company's response.'**

## RISK REPORTING

**'You need to get the right balance between the report containing enough detail to be useful and being at a sufficiently high level to be manageable for non-executives.'**

From our interviews, it was clear that the role of risk management in a corporate, however it is organised, is to facilitate the management process of considering risk and making well-grounded decisions regarding its acceptance and mitigation. Formal processes of risk identification and reporting were almost universally used, recognising that they were not an end in themselves but a means to the end of better management decision-making. Many also acknowledged that even a good risk reporting process suffers from the fact that no-one can ever foresee everything : **'…often our managers can be more risk averse than the board. It's the risks no one considers that are the problem, rather than the risk not being communicated.'**

More than 80% of companies surveyed have a process that requires risks to be identified in a structured fashion at least twice a year, and often more frequently. See Fig. 16

The great majority of companies (87%) used an enterprise-wide risk management process to integrate the picture of risk and risk management across the business. This was the case regardless of whether or not they had a separate risk management function or a CRO. About the same proportion used specialist risk management software for maintaining a risk register; about two-thirds of these had been developed internally and the remainder were external solutions.

Heat maps are widely used. Some interviewees were slightly dismissive of 'brightly coloured pictures' but more said that they found them useful for giving an insight into what was going on in the business, not merely as the output of the risk management process.

>>>

**Make the compilation of a risk register an integral part of project planning, contract signing or process management.**

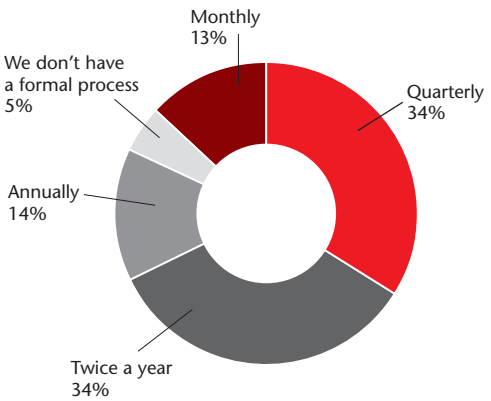



Fig. 16 (Factual questionnaire)
**How frequently does your risk management process require risks to be identified in a structured way?**

## THE DANGER OF STALENESS

**'It gets stale as the process is repeated annually… the biggest challenge is keeping it alive.'**

While risk identification and reporting processes are widely used, a substantial number of interviewees highlighted the danger that they can quickly become stale, with the consequence that they become formalities rather than something actively used to help run the business better. There were two main remedies for this.

One was to vary the process frequently, including varying the appearance of the documentation and the nature of the risk identification discussions, so that people have to approach it as something new.

**'Having the CEO leap around with a pack of Post-It Notes made the process come alive and set the attitude for the rest of the business – it was transformational.'**

The other was to focus the risk identification and reporting process on the risk consequences of change, both in the outer world and within the company.

## RISK APPETITE

**'It's not very relevant to have a statement of risk appetite – it's a question of keeping on top of risk exposures all the time.'**

**'Risk appetite is a valuable concept but trying to do it in terms of financial impact is tricky.'**

**'The board have not explicitly stated their risk appetite except perhaps in the context of acquisitions… appetite must depend on the nature of risk. It is more about demonstrating attitude to risk.'**

All those we interviewed were familiar with the concept of risk appetite. Familiar enough, indeed, to be able to say in the survey that they did a good job with it. However, interviews showed that few regarded a single expression of risk appetite as being relevant to their businesses, and although the term risk appetite was used in conversation it was rarely part of a company's formal terminology. By and large this was because interviewees understood risk appetite to mean the quantitative expression of the risk that a company is prepared to take on, expressed in terms of financial impact. Corporates' operational risks are usually both numerous and diverse, and many do not lend themselves to financial measurement. So it is not practical to obtain a single number, or even set of numbers, to represent acceptable financial exposure from risk; and in consequence it is dismissed, at least as a management tool if not as a concept.

What interviewees found valuable in the concept could better be described as 'attitude to risk'. This is something which is implicit in every board decision, a point made by many of those interviewed. By being consistent in its approach to decision-making, a board communicates its attitude to risk. This provides an explanation for why, despite the fact that few companies actually use the term or have formal statements of it, 92% of non-executives surveyed thought that their boards were good at agreeing a clear statement of the company's 'risk appetite' and over 61% of management felt that their boards were effective in holding them accountable for keeping to agreed risk tolerances.

Communication of its attitude to risk is necessary if the board's 'tone at the top' is to have any effect on the organisation below. However, implicit communication is more prone to misunderstanding, particularly by those more remote from the board. The substantial divergence between the NED and executive responses in the previous paragraph certainly suggest that not everyone is on the same page.

It may be desirable for boards to give more explicit communication to managers of their attitudes to risk,

>>>

**Don't have 'risk workshops' or 'forums'. Position them as opportunities to reflect on the business.**

**Rather than trying to quantify reputational risk, think in terms of duration – how long will you tolerate bad publicity?**

**Try talking about 'risk intolerance'.**

**Periodic 'deep dives' by the audit committee send a message about risk attitude.**

**Use 'war stories' to make messages relevant and practical.**

in the form of narrative descriptions of risk appetite without emphasis on quantification. This can partly be done by communicating explicitly how this has influenced board decision-making. Some organisations express their risk attitude by making it an integral part of their value statement and 'ethos' for doing business.

Some effort in this regard would command reasonable support: 64% of management and 45% of non-executives surveyed agreed that more resources could be invested in communicating the board's risk appetite.

## TURNBULL

**'The Code per se does not increase confidence – people and their behaviours do.'**

A substantial minority of NEDs surveyed were doubtful about the usefulness of both Turnbull and the annual review of internal control effectiveness. See Figs. 17 and 18

Management put Turnbull relatively low on the list of things that they would like to spend more on, with a much stronger preference for increasing the consistency of risk management across the business. See Figs. 19 and 20

Fig. 17 (NED questionnaire)
**The Combined Code ('Turnbull') process gives the board confidence that the internal control and risk management processes are working well.**

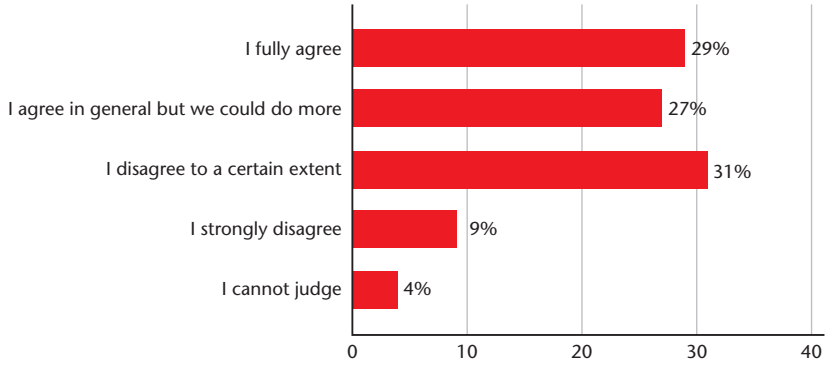



Fig. 18 (NED questionnaire)
**The Combined Code ('Turnbull') process is a compliance excercise that adds little value to ensuring that key risks are identified and managed.**

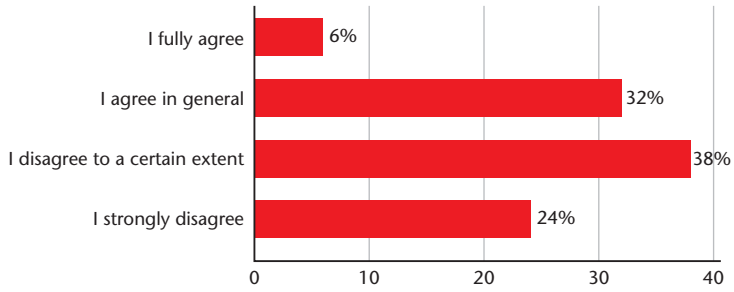



Fig. 19 (Management questionnaire)
**If I had more resources, I would invest more in the Combined Code ('Turnbull') process to give me additional confidence that the internal control, risk identification and risk management processes are working well.**

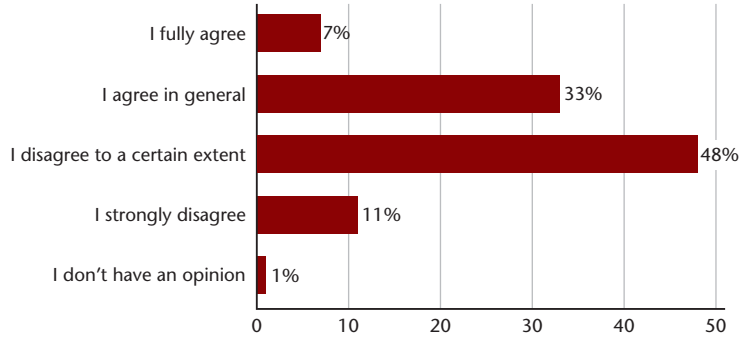
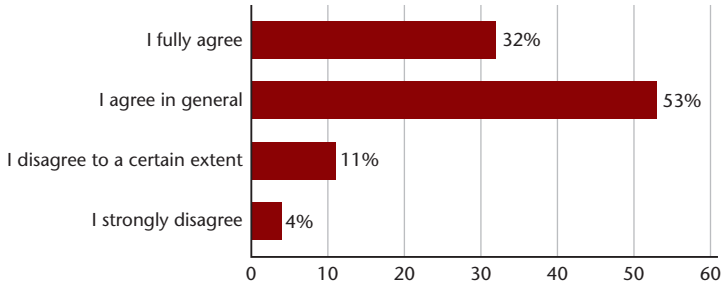


Fig. 20 (Management questionnaire)
**If I had more resources, I would invest more in ensuring that the quality of risk management is consistent across the business.**




However, a more positive flavour emerged from the interviews, which indicated that the principles set out in the *Turnbull Guidance on Internal Control* remain relevant. The annual review of internal control effectiveness was thought by many to be a useful discipline, albeit sometimes something of a formality, and in a few cases it was used as the basis for a wide-ranging review of risk and control. It would seem that for Turnbull, as for the rest of the Combined Code, its usefulness depends on how people implement its principles.

## HEALTH AND SAFETY

**'Safety is something of a bellwether – if this is good or bad, it usually indicates management strength or weakness more widely.'**

For a substantial proportion of companies interviewed, Health & Safety (H&S) is one of the most significant operational risks. In most cases, it was the subject of oversight by the whole board, with H&S reporting coming high on the board agenda.

A few interviewees suggested that a good H&S culture was an indicator of a good risk management culture more generally. As our interview programme went on, an overall impression began to form in the minds of our interviewers that there did seem to be some connection. However, detailed analysis of the interviews and the survey results did not yield convincing evidence one way or the other.

It may be that, although a good H&S culture does not of itself bring about good risk management, it can help to create a disciplined environment which is responsive to risk management initiatives. If this were so, one implication would be that companies which do not face significant H&S risks, a category which includes financial services organisations as well as many corporates, may need to work harder than others at embedding a strong risk culture.

This is an interesting point for which more evidence is required and it would merit further research.

## REWARD

**'Accountability feeds through to reward with a direct link into the performance rating – but embedding into the culture is more important than tying to reward systems.'**

In none of the companies that we interviewed was reward seen as a major element of the risk management system. While a few felt that more could be done to use performance reviews to embed risk management, others felt that it was too complicated to be effective.

In general, performance-related pay was said not to be a substantial element of reward below senior executive level, and was therefore not thought to be a significant motivating factor; and a number of companies had recently adjusted their reward systems in order to make it even less so[13]. Nor was it thought that reward systems created significant risks except in relation to well-understood areas such as revenue recognition, which companies managed by means of audit and counterbalancing KPIs.

However, there were a considerable number of companies where those to whom we spoke were rather vaguer on this topic than we might have expected. This suggests that there are opportunities for audit committees, in particular, to develop a better understanding of the risks and opportunities arising from reward systems.

13 It was outside the scope of this project to explore why, if performance-related pay is not a significant motivating factor, it is worth having at all.

# THE GHOSTS OF CRISES PAST, PRESENT AND (MAYBE) FUTURE

**'The company had been very sick. The people at the top were wrong, and those in the middle had given up… now one of the signs that things are better is that managers are willing to tell the board when things are not right.'**

A number of companies interviewed had within the last few years undergone some sort of major crisis which had caused a reassessment of their risk management. Actions taken included at least some, and often most, of the following:

- changing the senior management
- increasing the strength of the board, particularly by bringing in more relevant experience
- greater emphasis on staff training and on embedding ethical values
- introducing improved risk ownership and risk identification, including more attention to 'spotting icebergs'
- improving the risk reporting processes, with better facilitation to obtain the buy-in of managers below executive level
- strengthening internal audit.

These changes are mainly about people and about doing better what was already in place. In only one case had it been found desirable to introduce a new board committee or make structural changes going beyond what is currently set out in the Combined Code. Otherwise, the changes focused on management, people and culture issues, and improving processes both to give better accountability and to make it easier for people to do the right things.

In relation to the present economic crisis, just under half of executives surveyed said that they were reviewing their risk management approach. However, only 31% said that they were likely to invest more in risk management. See Figs. 21 and 22

>>>

**Revisit big decisions and major transactions, be honest about them, build the learnings into corporate wisdom.**

Fig. 21 (Management questionnaire)
**The fallout from the current financial/economic crisis is leading us to review our risk management approach.**

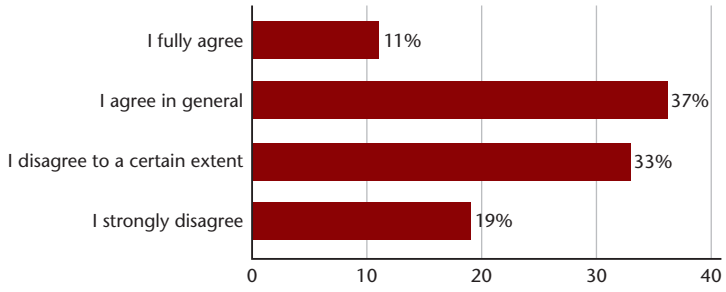
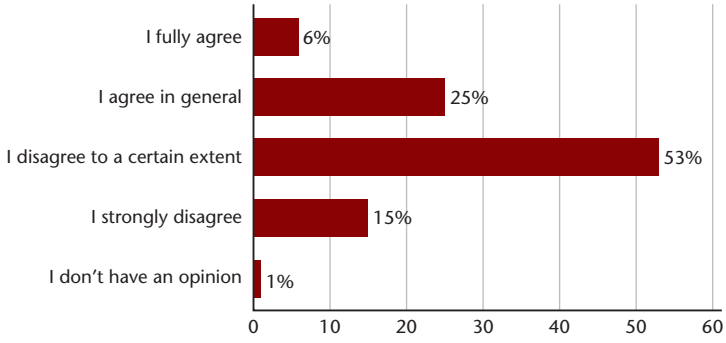



Fig. 22 (Management questionnaire)
**The fallout from the current financial/economic crisis is likely to result in us investing more in our risk management approach (or has already caused this to happen).**



From interviews, it was clear that there was in fact no inconsistency in companies' responses. More time and attention are being given to consideration of risk by both management and boards, but from within existing resources and without major organisational changes. Events in the financial services sector do not appear to be generating a feeling that significant changes to risk management practice are needed. Companies realise they need to think more rigorously about risk, but achieving this is a matter of focus and discipline, rather than additional people or new organisational structures.

The main areas of increased focus included:

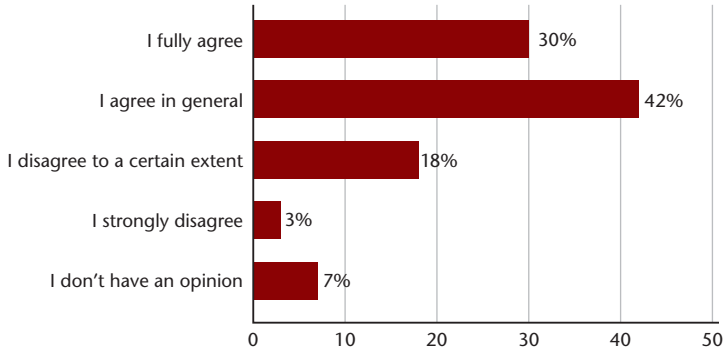
- financing, liquidity and covenants
- supplier and customer stability
- the potential for a major risk to emerge from combinations or sequences of individual ones
- legal and compliance.

Almost three-quarters of managers surveyed said that the board was effective in debating risk scenarios.
See Fig. 23

However, interviews showed that very few companies actually used formal scenario planning. Although some used the term, what most were actually doing was stress testing their business plans and financial forecasts, most often in relation to covenants and cash flow.

Most companies recognised the need to build resilience into their business and financial models in order to allow for the unforeseen. Only a minority expressed it in explicit terms, with the remainder leaving it under the more general heading of 'being more risk-averse'. There is room for some companies to improve their risk management by being more explicit about the fact that not all risks can be identified and the need to build in some degree of resilience to cope with unexpected shocks.

Fig. 23 (Management questionnaire)
**The board is effective in debating risk scenarios.**



# SHAREHOLDERS ETC

**'…not a huge amount of interest in risk management from investors. They are only interested when things go wrong.'**

A question which put investment analysts in a positive light generated one of the biggest 'strongly disagree' responses in the entire survey.[14] See Fig. 24

The interviews were even less favourable than the survey responses. Almost all those interviewed had expectations that were about as low as they could be. With the occasional honourable exception, investment institutions were seen as both inexpert and uninterested in a company's risk governance, or even in the risk involved in its strategy. A handful of interviewees recounted positive experiences with shareholders, but a greater number complained that during the boom times they had experienced investor pressure to take on risk (particularly more financial risk through increased leverage).

A number of interviewees emphasised that major shareholders tend to have very different investment objectives and time horizons, which makes engagement difficult even when they are interested.

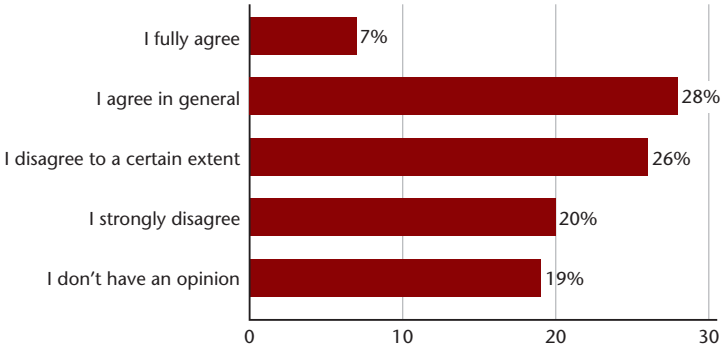
The subject of engagement with shareholders tended to generate strong feelings. Often these seemed to be based on frustration, which is at least better than indifference.

We also enquired about others involved in the provision of capital but few interviewees could remember any of them showing much interest in risk governance. Perhaps most revealingly, 29% of survey respondents had no opinion on the rating agencies' understanding of their risk management approach, and few of those interviewed seemed to make any mental connection at all between rating agencies and risk governance. These results suggest that the agencies have not been asking particularly memorable questions in this area.

One company in a particularly capital-intensive industry said that they had obtained better pricing on loans after demonstrating the effectiveness of their risk management to the lenders.

Another mentioned that they had obtained a reduction in their directors' and officers' liability premium as a consequence of explaining their risk governance.

**Fig. 24** (Management questionnaire)
**The investment analysts in general show an active interest in and a good understanding of our risk management approach.**




14 Beaten only by management's lack of enthusiasm for increasing internal audit headcount and investing more in risk management as a group function.

# PRIORITIES FOR BOARDS

**This report contains a large number of ideas and suggestions for how boards can improve their risk governance. Not all will be applicable to every company. But in this section we summarise what we think are some of the most important things for a board to watch out for.**

- The natural human bias to optimism, which has to be consciously – and uncomfortably – resisted.
- Strong, hands-on managers, who (even if they are very good) might not see the need for the more formal processes that NEDs need if their oversight is to be effective.
- A culture – in the boardroom and beyond – where people are reluctant to admit mistakes and don't welcome challenge.
- Directors having inconsistent expectations regarding their role and what they can reasonably be expected to accomplish.
- Leaving too much to the audit committee, so that some directors aren't involved in 'board-level risk acceptance'.
- Confusing an executive risk committee with a board oversight committee.
- NEDs not getting out and about enough to really understand the business and its people.
- Board papers and other aspects of board process that cause NED time to be spent unproductively when they could be getting out and about instead.
- Insufficient breadth of expertise around the board or audit committee table to be able to understand the whole range of significant risks facing the company.
- NEDs' trust in management being insufficiently grounded and hard to defend.
- An audit committee and a remuneration committee which each thinks the other is dealing with the risk arising from reward schemes.
- Not thinking hard enough about the unexpected and the need for resilience.
- Not communicating a consistent attitude to risk and mitigation, and not knowing if the troops are actually hearing and understanding what the board thinks it's saying.
- A CEO who doesn't give a clear lead about the importance of risk management or who isn't a visibly strong sponsor of internal audit.
- Indistinct accountability and unclear policies.
- Risk processes becoming mechanical and static.

# ACKNOWLEDGEMENTS

## COMPANY PARTICIPANTS

Aggreko plc
Amec plc
BAE Systems plc
BBA Aviation plc
BG Group plc
Bovis Homes Group plc
BP plc
British Airways plc
BT Group plc
Burberry Group plc
Cairn Energy plc
Compass Group plc
Cookson Group plc
The Davis Services Group plc
Debenhams plc
Diageo plc
Daily Mail and General Trust plc
DS Smith plc
EasyJet plc
Electrocomponents plc
Eurasian Natural Resources Corporation plc
Filtrona plc
GlaxoSmithKline plc
Halfords Group plc
Hays plc
Home Retail Group plc
Imperial Tobacco Group plc
Inchcape plc
Inmarsat plc
International Power plc
J Sainsbury plc
Kingfisher plc
Land Securities Group plc
Liberty International plc
Mitie Group plc
Morgan Sindall plc
Mothercare plc
N Brown Group plc
Pearson plc
Premier Farnell plc
Reckitt Benckiser Group plc
Rio Tinto plc
The Sage Group plc
Severn Trent Water plc
Shaftesbury plc
Smiths Group plc
Spirent Communications plc
Stagecoach Group plc
Stobart Group Limited
Tate & Lyle plc
Tesco plc
Ultra Electronic Holdings plc
Unilever plc
United Utilities plc
Vodafone Group Plc
Weir Group plc
Wm Morrison Supermarkets plc
Wolseley Group plc
Xstrata plc

## HELPERS AND ADVISERS

A large number of people gave generously of their time to help with this study, whether by completing the survey, being interviewed, or both. Independent Audit Limited and The ICAEW Foundation are very grateful to them all.

In addition, we would like to give special thanks to the following:

Sir Christopher Hogg, Chairman of the Financial Reporting Council, for writing to FTSE chairmen to ask for their participation in this study – without this we would never have achieved such wide coverage

Norman Murray and Ian Harley, who were consulted during the planning of this study and let us try out questionnaire ideas on them

The Reporting and Public Policy Team at Ernst & Young, for their detailed comments on the questionnaire content

Professor Michael Power of the London School of Economics, for acting as our research adviser and providing helpful feedback, always at very short notice

Xinyi Zhang and Ruth Kaufman, both also of the London School of Economics, for their help with the statistical analysis

Eric Anstee of The ICAEW Foundation, Michael Izza of The Institute of Chartered Accountants in England and Wales, and Steve Maslin of Grant Thornton, for acting as project governance committee; they managed both to be practically helpful and to keep us more or less on schedule, but without being interfering

Nick Handy, who acted as our quality reviewer, making sure that every assertion was underpinned by good quality evidence. In the unlikely event that any errors have survived his eagle-eyed scrutiny, they are the responsibility of Independent Audit Limited alone.

## SPONSORS

**The ICAEW Foundation is immensely grateful to the following sponsors for their generous contributions towards the cost of producing this report:**

**Admiral Group plc**
**Amec plc**
**Amlin plc**
**BDO Stoy Hayward LLP**
**BG Group plc**
**British American Tobacco plc**
**The British Land Company plc**
**Cable & Wireless plc**
**Deloitte LLP**
**Ernst & Young LLP**
**Friends Provident Group plc**
**Grant Thornton UK LLP**
**KPMG LLP**
**Liberty International plc**
**Lonmin plc**
**PricewaterhouseCoopers LLP**
**Reckitt Benckiser Group plc**
**Smiths Group plc**
**Wm Morrison Supermarkets plc**

## The ICAEW Foundation

Launched in 2007, The ICAEW Foundation is designed to shape the future of the profession by creating life-changing opportunities for the disadvantaged, ground-breaking research that inspires business confidence and closer ties between academia and the profession.

To find out more or to make a donation, please contact the foundation at the address below.

## Independent Audit Limited

Independent Audit Limited is a specialist board and governance consultancy. We help boards know that their governance is working well. We understand what boards need and how businesses work, so we get to the big issues without fuss and suggest straightforward, practical improvements. We work with organisations of all shapes and sizes and in all sectors.

**The ICAEW Foundation**
Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK
**T** +44 (0)20 7920 8647 **F** +44 (0)20 7920 8457 **E** foundation@icaew.com **www.icaew.com/foundation**

Registered Charity No 313983

MKTPLN8703