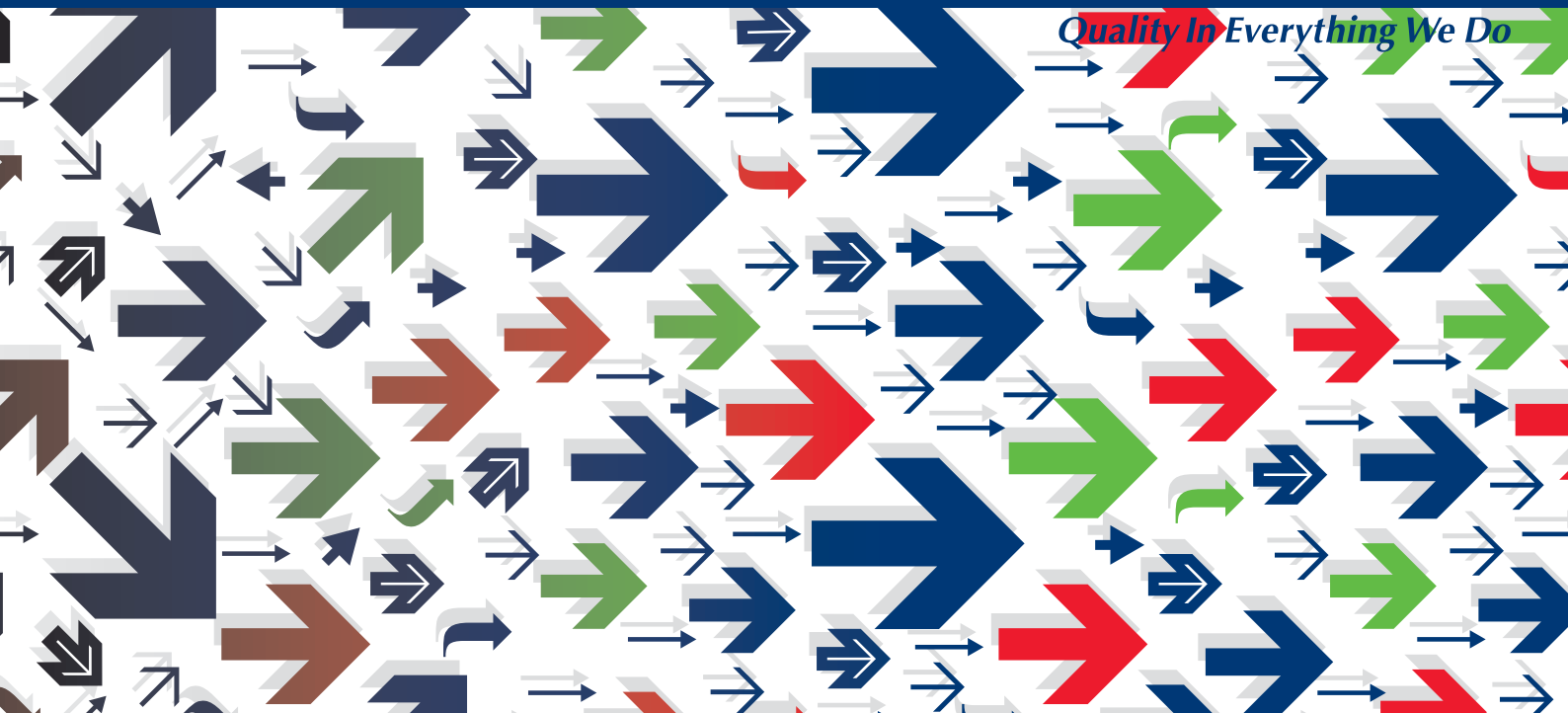


Risk Management

What do Independent Directors do?

 ERNST & YOUNG

Quality In Everything We Do



Risk management: What do Independent Directors do?

Introduction	2
Overview of findings	3
The research	3
1 Findings	4
Committees and meetings	
2 Who does what in risk management?	5
Key thought	
Regulatory background	
What we discovered	
3 How do you set your risk appetite?	9
Key thought	
Regulatory background	
What we discovered	
4 The dangers of standardisation	11
Key thought	
What we discovered	
5 The impact of the business review	12
Key thought	
Regulatory background	
What we discovered	
6 How 'better practice' emerges	14
Key thoughts	
Regulatory background	
What we discovered	
7 What's the biggest problem you face?	15
In conclusion	17
Questions to ask yourself?	17
Appendix	18
Acknowledgments	18

Introduction



Gerald Russell
Senior Partner – London
Chairman, Independent Director Programme
Ernst & Young LLP

It is hardly surprising that, at a time of considerable economic uncertainty when risks for businesses in the global market place are increasing, boards and independent directors (IDs) in particular should worry about the risks they and their businesses face. How can they ensure those issues are properly assessed and managed?

In our annual research for independent directors in 2007 (Why does the strategic agenda remain elusive?) there was a very clear message that IDs were uncertain as to both their role in risk management and, perhaps more to the point, how they should discharge their duties. So this year we decided to undertake an in-depth study into how IDs deal with this issue on the ground.

Our survey achieved excellent coverage which extended to 96 listed companies, over 60 of them in the FTSE 350.

I suppose the result that we obtained should not really be that surprising. In short, how IDs approach the question of risk management in their companies is highly variable. There appears to be no one particular way, method, policy or process which seems to permeate across those businesses. Indeed, those directors who sat on multiple boards contrasted the differences in practice that they had come across. No doubt this is because all companies are different and appetite for risk is different; thus what is acceptable risk-taking in one would not be in another.

So what do IDs really rely on in terms of appropriate risk management? The answer to come very strongly from this research is that it is all down to culture and tone from the top. And, of course, culture is extremely difficult to assess objectively. It is all about trust and feel. It is this highly subjective flavour that our IDs considered to be far more important than risk registers per se. Indeed, too much focus on the mechanics of the risk register could lull IDs into a false sense of security, believing that because risks were being listed, they were also being managed. That's a very different thing.

The whole point here is that the Turnbull guidance does not prescribe one way of managing risk or assessing it. It calls for 'Review'. Even in the highly process-orientated and regulated world that boards operate in, IDs are often significantly reliant on their own assessment of the culture of an organisation. This determines the degree of trust they place in the executive management to run the business in a sensible risk-taking but also risk-controlled way. At the end of the day that is after all what they are there for.

There is no silver bullet. I trust you find the concerns, thoughts and practices that come out of this research helpful in framing your approach.

A handwritten signature in blue ink, appearing to read "Gerald Russell".

Overview of findings

Agreement on where responsibility lies	The ultimate responsibility for risk management lies with the Board, but the practice of risk management is the responsibility of the executives.
No common model	There is no single way of configuring the Board and its committees to deal with risk. Although financial risk is dealt with by the audit committee, a variety of structures was in existence to manage non-financial risk and to create the underlying risk registers.
Culture is key	There was agreement that effective risk management depends on there being an appropriate culture of risk-awareness throughout the organisation.
Reliance on executives	Independent directors are heavily reliant on the competence of their executive colleagues, and need to feel that they can trust them.
Risk is the flipside of opportunity	Businesses need to take risks in order to make profits. Risk cannot be managed away; the important thing is to understand the degree of risk being taken.
Outside the financial services sector, risk appetite is not clearly defined	Banks and financial services companies quantified the risks they were prepared to take, as part of their business strategies. For non-financial companies the risk appetite was more qualitative, gut feel, and unspecified.
Risk management is context-specific	Different risks are important in different industries and at different stages of the business lifecycle.
'Better' practice develops through interaction with peers	Practices are carried between companies through independent directors' membership of several boards, and through their interaction at seminars and conferences.
Business Review may cause competitive problems	Some participants were concerned that the need for additional disclosure in the business review would put them at a competitive disadvantage.
Disclosure sometimes drives practice	The requirements for additional disclosure in the business review have led some companies to upgrade their risk management practices. For others, the review just codified current practices.
Ticking the boxes can be dangerous	Although it is important to have a risk review and management process, too much focus on process alone could provide a false sense of security to the Board.

The research

The research contains the views of 42 independent directors (IDs) from a cross-section of FTSE 350 companies.

Between them, these individuals had 102 independent directorships of listed companies, sitting on 96 Boards.

The 42 participants sat on 84 audit committees, of which they chaired 43.

Early findings of the research were discussed in a roundtable focus group with 4 participants.

Further details of the research are given in the Appendix.



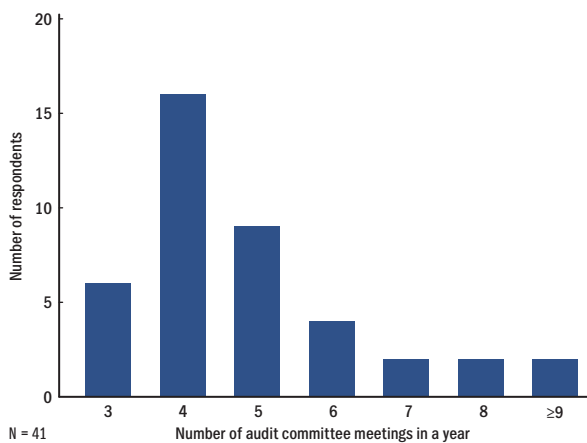
Findings

The research was based around a series of questions regarding how IDs and their companies viewed risks and how those risks were identified and controlled. The key learnings are captured below. Where relevant we have included a brief overview of the regulatory background to the topic.

Committees and meetings

In the questionnaire, participants were asked how many meetings their audit committees held in a year, and how and why this had changed over the past three years. Charts 1 and 2 show that overall the number of meetings has risen, with the main reasons being the increase in the work required of the audit committee (which includes more work on risk review), increased reporting requirements, and a move towards 'better practice', entailing more extensive consideration of the issues.

Chart 1a Numbers of audit committee meetings



A majority of audit committees have more than four meetings a year, but four is the most common number.

Chart 1b How has the number of audit committee meetings changed over the last three years?

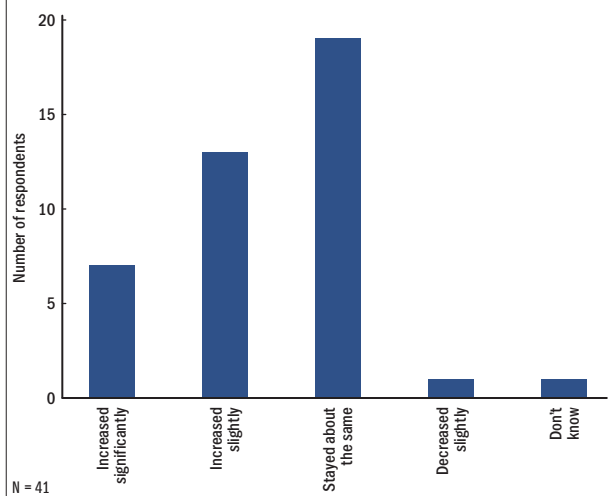
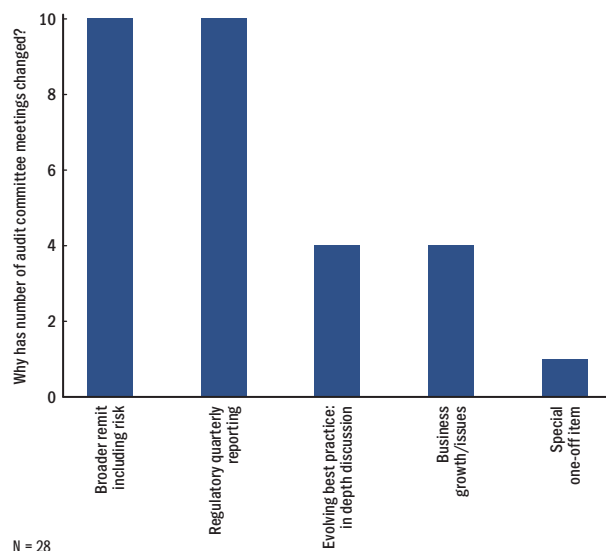
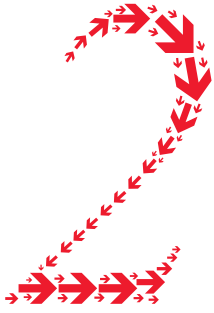


Chart 2 Reasons for change in number of audit committee meetings





Who does what in risk management?

“... the NEDs' [non executive directors'] role is to try and make sure the execs understand risk. The execs' job is to ensure they manage the risks. ... the NEDs make sure they are satisfied that the execs have been rigorous in this process. In my opinion if the execs do not take ownership and manage the process, then it is not embedded. Risk management is an exec function and responsibility.”

Audit committee chairman, FTSE 250

Key thought

The one very clear finding about risk management within the companies under discussion was that there was no standard way of approaching it. The division of responsibilities between Boards, audit committees, risk committees and executives varied between organisations. Processes reflected variants of top down and bottom up analysis, and different aspects of risk were treated in different ways. In part this appeared to be a function of the different industries in which the businesses operated, and in part it reflected each company's history and culture, and the individual preferences of the protagonists.

Regulatory background

The Combined Code sees risk assessment and management as part of the role of an effective Board, and charges the independent directors with ensuring that supporting systems are robust. Further to this, the Smith Guidance provides recommendations on the work of audit committees, and their role in dealing with risk. Extracts from both documents are shown in Box 1.

Box 1 The Board, the audit committee and risk management

Extracts from the Combined Code (2006)

Main principle: Every company should be headed by an effective board, which is collectively responsible for the success of the company.

Supporting principles include: Non-executive directors should scrutinise the performance of management in meeting agreed goals and objectives and monitor the reporting of performance. They should satisfy themselves on the integrity of financial information and that financial controls and systems of risk management are robust and defensible.

Extracts from the Smith Guidance

The audit committee should review the company's internal financial controls (that is, the systems established to identify, assess, manage and monitor financial risks); and unless expressly addressed by a separate board risk committee comprised of independent directors or by the board itself, the company's internal control and risk management systems.

The company's management is responsible for the identification, assessment, management and monitoring of risk, for developing, operating and monitoring the system of internal control and for providing assurance to the board that it has done so. Except where the board or a risk committee is expressly responsible for reviewing the effectiveness of the internal control and risk management systems, the audit committee should receive reports from management on the effectiveness of the systems they have established and the conclusions of any testing carried out by internal and external auditors.

Guidance On Audit Committees, 2003 (The Smith Guidance) Paras 4.5 and 4.6

What we discovered

“It’s the managing of the risk that counts, not whether you’ve done it in a particular way.”

Independent director, FTSE 250

It was generally agreed that the ultimate responsibility for risk management lies with the Board, but that the practice of risk management has to be the responsibility of the executives.

There was no standard way in which the companies approached risk management. Eleven of the interviewees gave brief descriptions of their companies’ approaches to compiling the risk register; of these, four had a mostly bottom-up approach and seven used both top-down and bottom-up. None of the participants had adopted an exclusively top-down approach to risk assessment, there was always an element of evaluation from lower levels of the organisation.

“... I start off with the head of internal control and ask what goes on. It goes to the risk committee – mostly finance people, who swear that they always talk to the general managers [so that risk does not have a purely financial focus] ...”

Audit committee chairman, FTSE 100

Although financial risk is dealt with by the audit committee, non-financial risks, which formed the bulk of our discussions, were handled in many different ways. Box 2 gives one example.

Box 2 Dealing with Health & Safety risks

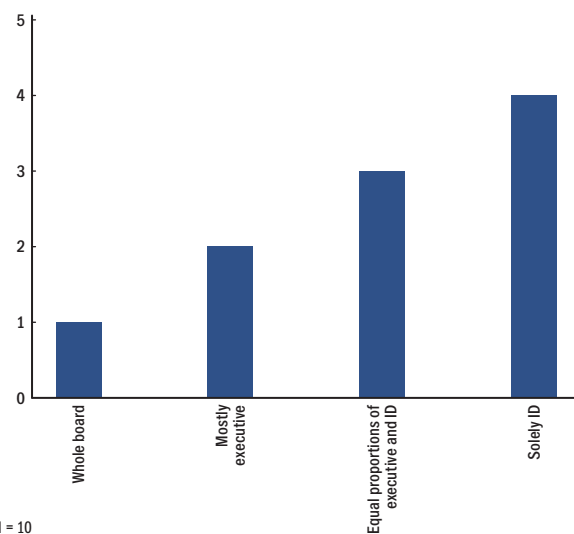
Health and Safety (H&S) risks were mentioned by 17 of the interviewees. In many businesses, particularly the extractive industries, construction and travel, this was seen as an area where there could be no tolerance for error.

In only one of these 17 companies was H&S under the remit of the audit committee. Five of them dealt with it directly at Board level, and 11 put into either a general risk committee or a dedicated H&S committee. These committees mostly reported direct to the Board, and often included both executives and non executives in their membership.

The division of duties between Boards, committees and executives varied. Most of the interviewees agreed that the buck stops at the Board, but that it would be impossible for the Board to consider each and every significant risk, and so that task was delegated. As stated, financial risk is a matter for the audit committee. In all but one of the companies some or most of the non-financial risk was also dealt with through the audit committee. However, strategic risk was mostly dealt with at Board rather than committee level.

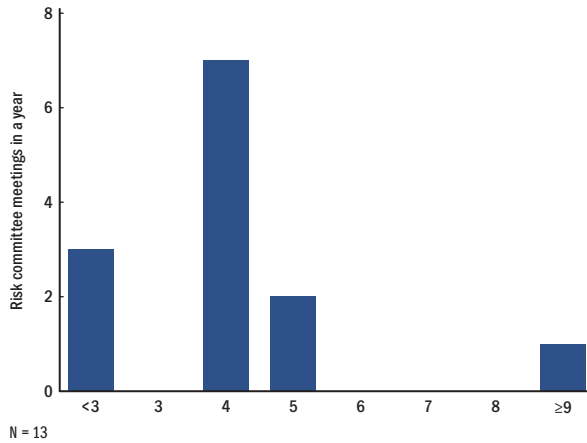
Eleven of the interviewees said that they sat on ‘risk committees’, although in two instances these were combined ‘risk and audit’ committees. Two individuals who did not themselves sit on risk committees were able to answer questions about how their companies’ risk committees operated. The majority of the committees reported direct to the Board, although in one instance such committee reported into the audit committee, and another reported to the chief financial officer (CFO). The composition of these risk committees is shown in Chart 3.

Chart 3 Risk committee composition



Risk committees, where they existed, varied in their composition.

Chart 4 How often the risk committee meets



Risk committees generally meet less often than do audit committees.

Many Boards approached risk management as an annual exercise, to be presented to the Board once a year unless circumstances changed. In some, there was an annual presentation but a rolling review (in committee) of specific risks on a programme throughout the year. Others had quarterly reporting. Board presentations were made variously by the chairs of the committees, the head of risk management, the chief executive officer (CEO) and the CFO.

Boards tend to look at summaries of the top ten risks. In one company, the Board saw 'the top 40-50 risks'; the ID who reported this said that in another of his companies the number considered was only the top ten, and a further Board on which he sat had a different process again.

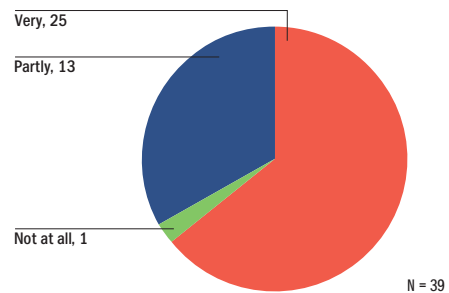
A problem with this, stated by several interviewees, is that by the time the risk register is summarised to the Board it has become very generic, and so the IDs may not appreciate exactly what is behind it. However, they felt that the constraints of time, as well as the lack of detailed understanding of the wide range of business issues, meant that this was probably inevitable.

IDs rarely delved into the detail of risk assessment and management, unless they had a particular interest in an area. The role of the ID was generally seen as being at a higher level, comprising review, and their job was to ask whether processes were in place rather than to go and test those processes. Having said this, some interviewees did refer to instances where they had probed further for information. Practices varied, and several interviewees commented upon the need for the IDs to have contact with the tier of management immediately below the Board, in order to get a better feel for what was going on. A few discussed risk management with several management tiers below the Board.

The IDs and committees placed a lot of reliance upon the role of internal audit in risk management. A majority of the respondents stated that their internal audit department spent more than a quarter of its time on operational matters, and that this had increased in recent years; only three stated that their internal audit functions just concerned themselves with the financials. In light of this significant role in risk management, it was seen as appropriate for the internal audit function to include, or to be able to call upon, a range of business experience rather than just comprising accountants.

Chart 5 Linking the internal audit programmes to risk assessment

How closely is the internal audit programme linked to risk assessment?



Almost all of the participants reported that their internal audit programmes were related to the organisation's risk assessment.

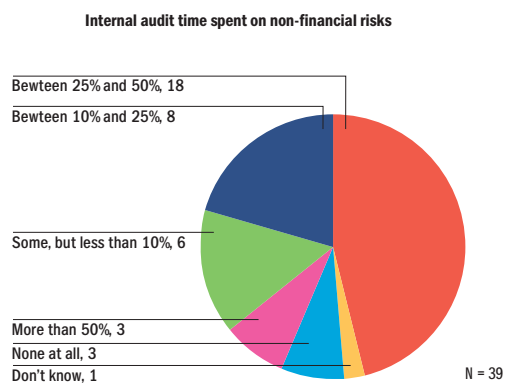
“It rarely requires us [IDs] to sally forth from the boardroom and go and look at a particular corner of the empire. We don’t go and check that the handrails are on every staircase . . . we treat our colleagues as grown ups.”

Independent director, FTSE 250, financial company

“It would be silly for me to have a look at it. It’s not why you employ NEDs, it’s why you employ [technical experts].”

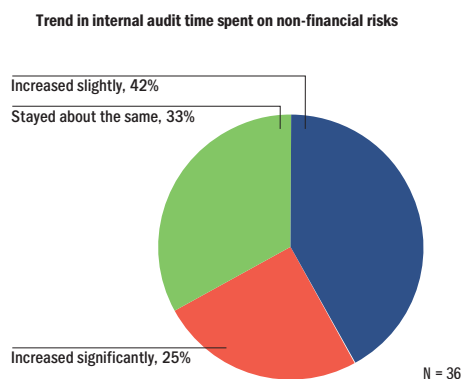
Audit committee chairman, FTSE 250

Chart 6 Time spent by internal audit on non-financial risks



The involvement of internal audit in assessing non-financial risks varied widely, but it most commonly took between a quarter and a half of their time.

Chart 7 Trend in internal audit time spent on non-financial risks



Over the past few years, none of the companies had reduced the time that Internal Audit spent on non-financial risks.

“It’s management’s responsibility to manage, and it’s our responsibility to ensure that the management process is in place. If that process fails, I’m looking for the CEO to answer for it, not the chairman of the audit committee.”

Independent director, FTSE 250

“You have to rely on the executive. You appoint someone to run a business; you don’t check every coal scuttle, knife and fork.”

Audit committee chairman, FTSE 250



How do you set your risk appetite?

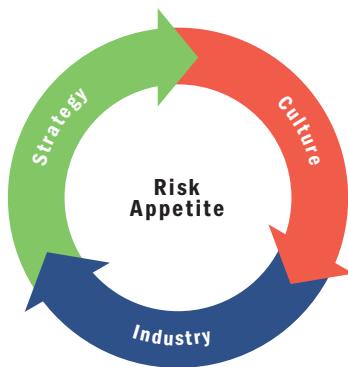
“Risk appetite is the degree to which we are prepared to take chances to make profit above the ordinary.”

Audit committee chairman, FTSE 100

Key thought

Companies need to take risks; it's how they make money. The level of risk considered appropriate – the 'risk appetite' – will depend on the company's industry, the selected strategy, and the culture of the organisation. Indeed, these three are inter-linked: decisions on strategy properly take account of the associated risks.

Box 3 Factors affecting risk appetite



The industry in which the company operates, the strategy adopted, and the culture of the Board and the organisation will all interact to influence the risk appetite.

Regulatory background

The revised 'Turnbull' guidance advises Boards to consider what risks are acceptable to the company, and to ensure that there is suitable guidance in place throughout the organisation.

Box 4 Turnbull requirements on risk appetite

Included in the appendix to the revised Turnbull requirements is a list of questions that a Board may wish to consider regarding risk and internal control. These include:

- Does the company have clear objectives and have they been communicated so as to provide effective direction to employees on risk assessment and control issues? For example, do objectives and related plans include measurable performance targets and indicators?
- Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis? These are likely to include the principal risks identified in the operating and financial review.
- Is there a clear understanding by management and others within the company of what risks are acceptable to the board?

*Revised Guidance For Directors On The Combined Code
Financial Reporting Council, October 2005*

What we discovered

For most of the companies under discussion, risk appetites are not formally set. Risk appetite reflected the company's history and culture, and came out of the business strategy. To a certain extent it also reflected the personalities of the protagonists, in particular the CEO. Sometimes it was an explicit part of the strategy-setting process, but in other companies the risk appetite was implicit. The exception to this was in finance and insurance companies, where the risk-return trade-off and risk-modelling are fundamental to the business model, and were considered in detail at Board level.

“How do you measure risk appetite? It's a bit like art: you know what you like.”

Audit committee chairman, FTSE 100

For non-financial companies there was generally felt to be an undefined and unwritten cultural norm within each company whereby the management and the Board were aware of what would be acceptable. Some of the participants stated that their companies were 'low risk' or 'conservative', although all set this in the context that a company has to take risks in order to make profits, and different industries inherently carry different levels of risk.

Risk appetite is a function of the company's business and strategy. Examples were given of companies moving into overseas operations, for example in China or the USA, where the Board appreciated that the risk profile would differ from existing business, and this was explicitly considered in determining strategy. In one instance, there was an as yet unresolved disagreement between a company's executives, who wished to take on a further level of commercial risk in order to win new business, and its IDs who thought this risk to be unacceptable. One participant in the focus group commented on this, stating that as a non executive you need to understand 'risks with the associated reward numbers attached'.

"It's difficult to talk about risk appetite in the abstract. If at the bank they came along and suggested this new product that would generate billions you'd know instinctively that that was risky. But difficult to quantify, although you might qualitatively try to place it on a 1 to 10 scale."

Audit committee member, FTSE 100 financial services

Several respondents pointed out that a risk appetite is very difficult to define, unless statistical probabilities can be assigned (which generally they cannot). A scale of 'low to high' is meaningless. As one said, "'moderate' means nothing". One person's 'low risk' activity might be another's risky endeavour. A telling illustration was given by one interviewee, comparing the experiences of several individuals traversing a narrow gangway between boats: objectively they all faced the same risk, but a few took it in their stride, some were uncomfortable, and others were truly scared.

"I would imagine all companies would actually end up saying their appetite is to take moderate risk, which really doesn't help at all. I don't think you can describe risk appetite at an all-encompassing level. You can only look at the specifics, e.g. tax risk, where you might want to take an 'aggressive' risk stance, but not so much that it might damage your reputation. It is therefore it is only around specifics that you can actually take a conclusion."

Independent director, FTSE 100

In establishing their approach to risks, a few of the interviewees discussed the 'traffic light' systems in use to highlight key risks. For example, two companies had broadly similar processes whereby the CEO and the Board established an overall risk appetite, which was then cascaded down the organisation. Each individual unit put together its own risk report, with the high-level summary coming back to the Board, colour-coded to show how each function was doing in each area. The focus of the independent directors could then be drawn to the critical areas.

Some companies looked at the risk register in slightly more detail. An example was a company where the top ten risks applying to the group were colour-coded, as were the top ten risks applying to each of the business units. Similarly, another organisation allocated risks between ten key areas, and colour-coded a report for the Board showing the top ten in each area.

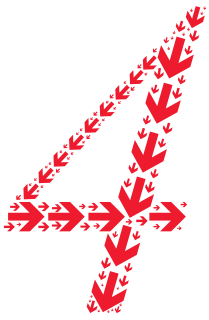
Variants of this system occurred, but most involved some sort of appraisal of the high-level risk register, whereby the IDs could see, for example, the nature of the risk, its potential seriousness, who was managing it and how. Further information could also be supplied, such as how the risk or its treatment had changed since the last time it was presented to the Board.

"It's about encouraging people to be more risky/adventurous, or to be less so, rather than saying that the risk appetite should be here, at this point on a scale."

Audit committee chairman, FTSE 250

"The return you get [profit] is for exposing yourself to a risk. You try to exercise your skills so that you manage that risk area better than your competitors."

Audit committee chairman, FTSE 250



The dangers of standardisation

“It’s dead easy to follow the paperwork, the perfect paper trail approach to risk – that’s an abdication of responsibility. Living the business model is more difficult.”

Audit committee chairman, FTSE 250

A view was expressed that risk management processes need to be embedded in the organisation, a fundamental part of the management systems rather than just an add-on for ‘good governance’ purposes. If the latter, risk management will just be a matter of ‘ticking the boxes’, rather than being a tool that managers can employ.

Key thought

Although it is important to have a risk review and management process, too much focus on that process could provide a false sense of security to the Board.

“You are in the hands of the executive for operating a process that is embedded. If the process is not embedded, if it’s just hanging on the side for governance reasons – that’s a problem. You need to ensure that it is embedded and adding value; if not, it’s pretty worthless.”

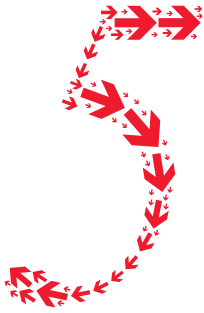
Audit committee chairman, FTSE 250

What we discovered

Although the need to formalise risk management systems was appreciated, three of the participants expressed a concern that having a system in place may lull Boards into a false sense of security that risk was all under control. They could also lead to a less creative approach to risk identification, which could be damaging. In other words, the act of writing up a risk register might be confused with the act of risk management.

“I am more keen on identifying key controls and debating how they are managed than going through a risk register.”

Audit committee chairman, FTSE 250



The impact of the business review

“The discipline of writing these things out can impact perceptions.”

Audit committee chairman, FTSE 100

Key thought

The need to formalise the presentation of risk in the business review has led some companies to review and revise their risk management processes; for others there has been no change. Some, but not all, companies fear that the additional disclosure requirements could result in competitive disadvantage.

“Its existence the [business] review brings risks up the agenda but [I] would not say that [I am] any more aware of risk than . . . previously . . . nor should the review have any impact in that way.”

Audit committee member, FTSE 100

Regulatory background

Although listed companies have been making narrative disclosures for many years, the statutory requirement for an enhanced business review in the Directors' Report has given the document a new scope and emphasis. Box 5 sets out the statutory requirements.

Box 5 Required contents of the business review

1. Fair review of the company's business
2. Description of the principal risks and uncertainties facing the company
3. Balanced and comprehensive analysis of the development and performance of the company's business during the financial year, and its year-end position
4. The main trends and factors likely to affect its future development, performance and position
5. Information on matters of corporate social responsibility such as environmental and employee matters
6. Analysis using relevant key performance indicators

Companies Act 2006 (s.417)

What we discovered

Reactions varied to the extended requirements to publish information about business risks. Some companies had changed their practices, others had not; some directors were concerned about the implications of reporting, others were not.

As regards the business practices, those companies reporting under US regulations have had to comply with the Sarbanes-Oxley Act for several years, and the directors saw no further issues arising from the business review. Similarly, directors from companies in regulated industries such as banking and insurance were satisfied that procedures did not need to be amended. Of the other companies under consideration, some had not changed their processes for risk assessment and management, but the business review had led others to reconsider processes. In these latter companies risk had moved up the Board agenda, processes had been formalised, and risk managers or directors had sometimes been appointed.

The implications of the additional public reporting proved interesting. To some it was a non-issue, but those who expressed concern did so for two reasons.

1. Competitive disadvantage

Some IDs were nervous that the additional disclosures would prove useful to competitors, as risk management was a fundamental part of their business model, and they did not wish to disclose detail of what they did.

2. Shareholder perception

Some IDs were concerned that extensive risk disclosures would concern shareholders and prospective shareholders, especially the less sophisticated investors, or those who did not understand the business very well.

“There’s a distinction between How are you going to run the business and manage the risks?, and What are you going to report?”

Audit committee chairman, FTSE 100

“It invites you to be more explicit about things you’ve dealt with implicitly in the past.”

Audit committee chairman, FTSE 250

Thoughts on the format and content of the business review were mixed. It was generally thought likely that some sort of boilerplate wording might emerge, and that practices would standardise around the leaders in each industry. Some thought this was a good thing, and were awaiting competitors’ published reports before they finalised their own disclosures. Other interviewees voiced the opinion that it would be a shame if this document took the legalistic form of, for example, prospectus disclosures: comprehensive, but hardly comprehensible.

“US companies will be lawyer-driven which will mean that all companies will end up going the same way and we will end up using the review as a boilerplate template of risks: which will be very generalised and which will make it meaningless.”

Independent director, FTSE 250

“The act of having to articulate anything does harden the responsibility. It doesn’t change the reality, but it often does harden the process and make you more aware. That’s a benefit.”

Audit committee chairman, FTSE 250

“But it’s going to be a case of ‘not frightening the horses’.”

Audit committee chairman, FTSE 250



How ‘better practice’ emerges

“It’s the strange process of non executive osmosis to spread hopefully better practice.”

Audit committee chairman, FTSE 250

Key thoughts

Practices that are found useful by one company are diffused throughout the corporate world through interlocking Boards, and through seminars and training sessions attended by IDs. However, this does not always happen – some of the interviewees discussed how practices differed considerably in the various Boards on which they sat.

Regulatory background

The Combined Code (2006) deals with the need for non executives to have a suitable induction into the company, and states that they should “regularly update and refresh their skills and knowledge”. The Smith Guidance extends this, as shown in Box 6.

Box 6 The need for ID training

Training should also be provided to members of the audit committee on an ongoing and timely basis and should include an understanding of the principles of and developments in financial reporting and related company law. In appropriate cases, it may also include, for example, understanding financial statements, applicable accounting standards and recommended practice; the regulatory framework for the company’s business; the role of internal and external auditing and risk management.

Guidance On Audit Committees, 2003 (The Smith Guidance) Para 2.19

What we discovered

Risk management practices, and IDs’ understanding of risk management can improve in several different ways. Fundamentally, these boil down to learning from company practice, and learning from peers and seminars.

In one of the companies under discussion the IDs had asked their executives to try to benchmark risk management practices against other companies in the UK (although this had not proved particularly easy to do). In addition to providing some comparators for the company’s own practices, this had also improved the IDs’ knowledge of the subject. A similar type of benchmarking, albeit internal, went on in some of the groups, where practices in many different subsidiaries were compared.

Training seminars put on by the Big Four firms of accountants were cited by most participants as a useful source of information on risk management. Attendance at such seminars varied between ‘occasionally’ and ‘often’. It was generally done at the ID’s own initiative – once directors had been inducted into their companies, there were rarely additional formal training sessions for Boards, although in two companies the in-house risk manager/director had put on a day’s training.

General reading, in terms of the business press and professional journals, was also considered useful in helping to keep up to date.

Externally-provided seminars disseminate best practice in two ways. The techniques discussed in the formal sessions are passed on, but also the networking with peers is a powerful means of picking up ideas for better practice, and one that was mentioned by most of the participants. Related to this, the IDs pointed out the benefits, to them and to their Boards, of sitting on the Board of more than one company, and so being exposed to different influences and ideas about how to approach the issues.

Having said this, and noted how practices diffuse amongst companies, the narrative earlier in this report concerning the diversity of practices shows that this diffusion is incomplete, perhaps due to the varying contexts in which companies operate, or their different histories and cultures.

“I would like all IDs to have a requirement to do CPD [continued professional development]. The extent of CPD undertaken should be specifically covered in the one-to-one meetings with the chairman as part of the board effectiveness reviews.”

Independent director, FTSE 100



What's the biggest problem you face?

“The worrying things are what you are not told.”

Independent director, FTSE 100, financial services

A final open question asked to all of the interviewees was, “What is the biggest problem you face as an ID looking at company risk?”.

By far the most common answers to this question revolved around issues of organisational culture, and trust in the executives. By definition, an independent director is not close to the operations of the business – their job is to stand back. Because of this they are reliant on the executives to brief them fully and appropriately, not only on current matters but also about emerging issues. All of the participants said that they trusted the executives with whom they worked, but many did express doubts as to whether they would be aware if their executives were less than open.

“As a non executive, the biggest problem generally is do I trust the integrity of management? It all comes down to that.”

Audit committee chairman, FTSE 250

Broadening this out, organisational culture was seen as critical. It is no use the Board setting out risk management policies if the people below Board level see it as an irrelevance and circumvent them. Part of the role of the Board – independent directors as well as executives – is to set a suitable tone for the business and to ensure that the appropriate attitudes to risk are embedded throughout the group.

Although some of the interviewees saw their role in risk management as taking place almost exclusively within the confines of the boardroom, others took a more proactive approach to trying to ensure that a culture of risk management was embedded within the organisation.

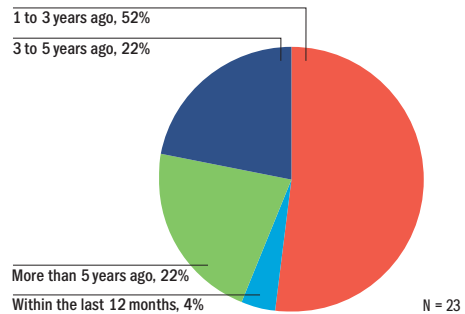
These individuals made a point of discussing the subject with a wide range of senior management, and tried to ensure that subsidiary boards had it as a regular agenda item. Further, when meeting management throughout the business, in different parts of the country and the world, they made a point of bringing up the topic of risk management – for example in terms of health and safety – as a signal of how significant it was to the Board.

Chart 8 Codes of conduct

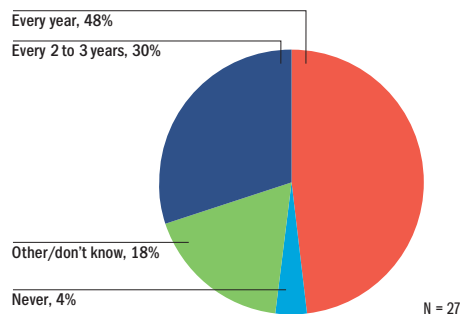
One way to help set the tone of the company is to have a formal code of conduct for employees. The questionnaire responses showed that 27 of the companies had such a code, 11 did not, and other respondents were uncertain.

Codes appeared to be a relatively recent development, and were reviewed regularly, as the tables below show.

When was your code drawn up?



How often is your code reviewed?



Major areas covered by the codes included business ethics, whistleblowing, general conduct, compliance with laws, fraud and health & safety.

The issue of ensuring that Board policies on risk management are followed throughout the organisation was highlighted by several interviewees as being even more critical in a multi-national company, which can reflect a collection of different cultural norms. Problems were also likely after acquisitions, where the culture and practices of the acquired business differed significantly from those of the purchaser.

“Choosing the right company is the biggest problem. Some companies may find it difficult to get IDs.”

Audit committee chairman, FTSE 100

“The biggest problem is not knowing the detail. At a high level, risk is easy to understand. But a lot of things will happen down in the detail of the business.”

Audit committee chairman, FTSE 250

“When tested in anger, I hope they [the controls] prove adequate. This is something I can’t judge nine times out of ten.”

Audit committee chairman, FTSE 250

Eighteen participants referred to issues of trust and culture, but in addition to that, the responses to this question were wide-ranging. Linked again to the position of the ID as removed from the day-to-day business of the organisation, it was a fear that they would fail to understand an aspect of the business, and so miss a risk, or that there would be a subtle change in the business environment or strategy, the ramifications of which passed them by.

One way in which IDs gained assurance in such matters was to take directorships in industries in which they had experience and thus understood the issues. Several individuals who had taken jobs in new sectors expressed a concern that it took a long time to become au fait with the ins and outs of the business.

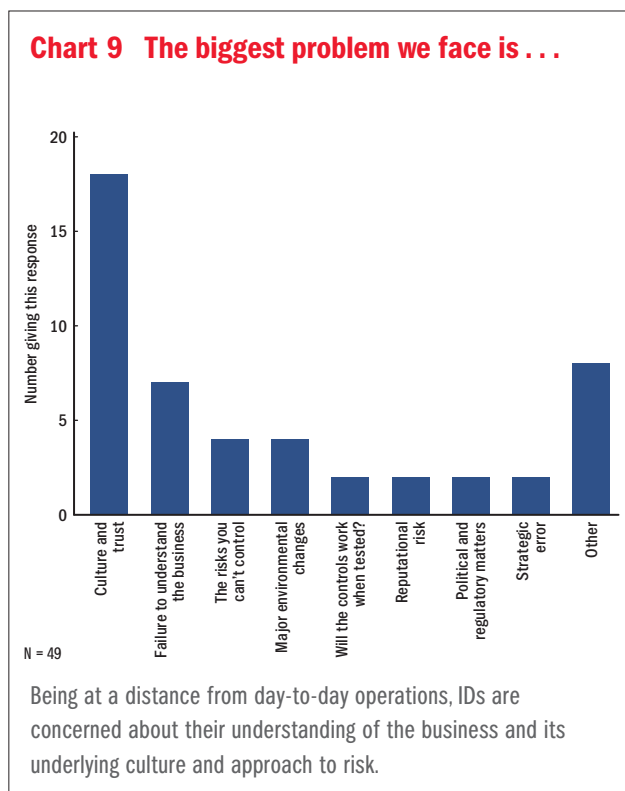
“But do you have the knowledge and experience to know which questions to ask to challenge the logic and [the CFO’s] explanations?”

Audit committee member, FTSE 100, financial services

Companies face many risks, some of which are outside their immediate control. Four interviewees stated that their biggest worry was the risks that could not be controlled, such as space debris crashing into a key operational site. It is necessary to consider how such a catastrophe would be approached. However, in practice most participants took the view that the focus in risk management should be placed upon those risks that can be managed, rather than these more unlikely occurrences.

“We tend to concentrate on last year’s risks, without necessarily worrying about what this year’s risks may be.”

Audit committee chairman, FTSE 250



In conclusion

Risk management is approached by Boards in many ways. A unifying concept is that the Board is responsible for ensuring that appropriate systems are in place, whereas the executives are the ones who undertake the practice of risk management. Within this over-arching approach, companies and Boards conduct themselves in different ways, with some Boards and independent directors being closer to the detail than others.

Taking risks is a necessary part of doing business, and none of the IDs participating in this research wanted to reduce their companies' risk appetite, although in at least one specific instance the IDs had a different opinion from the executives as to what level of risk would be appropriate. The risk appetite comes out of the company's industry and its strategy, as well as the personal views of those on the Board. It is rarely formalised (other than in financial services businesses where risk can be assessed statistically), but the IDs believe that the acceptable level of risk is understood by all concerned.

Inevitably, the independent director at a distance from the company's operations, relies on the executives to ensure that risk management is tackled appropriately. To do this, the ID needs to be able to trust the executives, but also must ensure that a suitably risk-aware culture permeates the organisation at all levels. These issues of trust and culture were amongst the most common concerns raised by interviewees: they are fundamentally important.

The practice of risk management is changing. In part, 'better' practices develop due to the interaction of independent directors with their peers, and their experience gained from being on several Boards. Increased regulation also drives development in practice.

For example, the introduction of the business review, in which companies will be obliged to set out their approach to risk, has tightened practice in some organisations, as the need for public disclosure has led to a reconsideration of the risk approach. However, for many companies the business review did not result in operational changes, as the Board took the view that practices were already sufficient. This was particularly so for companies listed in the United States, which have been in compliance with Sarbanes-Oxley.

One concern noted about changes in practice driven by regulation was that the need to 'tick the boxes' could lead to a risk management process driven by corporate governance requirements and divorced from the day-to-day operations of the business. It was emphasised that having a checklist, or a risk register, does not in itself provide a good tool to manage the risks faced by a complex organisation.

Questions to ask yourself?

1. Is there a logical reason for our company to manage risks the way it does, or has the structure just evolved through circumstance? Would it be useful to re-appraise risk management structures?
2. If the Board is delegating a lot of the work on risk to the audit committee, does the audit committee have too much to handle thoroughly? Is the audit committee becoming a surrogate Board for this purpose, and if so, does that matter?
3. What processes are other companies adopting that we could use ourselves?
4. Should we have a separate risk committee? If so, what would it do and who would be the members?
5. How do we ensure that we are not so focussed on 'ticking the boxes' that we fail to look at risk with a critical eye?
6. What are we doing to ensure that attitudes to risk are embedded throughout the organisation? How do we assess that the culture supports risk management?

Appendix

About the research

Independent directors from a cross-section of FTSE 350 companies were emailed and invited to participate in the research, either by completing an online questionnaire, or by agreeing to a telephone interview, or both. The final number of participants was 42, of whom 41 completed the questionnaire and one was interviewed without completing the questionnaire.¹

The research questionnaire was designed to elicit information about Board and committee structures regarding risk management, together with supporting data about how such practices had changed in recent years. Participants who sat on the Boards of several companies were asked to complete the questionnaire in respect of just one of those companies. The focus of the interviews was on the processes surrounding risk management, and the respective roles of the executives and non executives. Interviewees on multiple Boards spoke mainly about one of their companies but did on occasion describe how practices differed in others.

The interviews and questionnaires were completed between October and December 2007. In December 2007 the initial results were fed back to a small focus group comprising four of the interviewees and three partners from Ernst & Young, in order to explore the early findings.

The report accurately reflects the balance of views received. However, the nature of this type of research is that it gives a valuable insight into what individuals and companies are doing, but it is not generalisable to the population at large. Because of this, we have not listed out the numbers of participants taking each point of view.

¹ The interviews were conducted by four interviewers from Cranfield and from Ernst & Young. Three interviews were face-to-face, the others were by telephone.

Acknowledgments

Ernst & Young wishes to thank Dr Ruth Bender of the Cranfield School of Management for managing and co-authoring this report.

Ernst & Young also wishes to thank all the Independent Directors that participated in this research study.



Gerald Russell
Senior Partner – London

Chairman – Independent Director Programme
Ernst & Young LLP

Tel +44 [0] 207 951 3434
Fax +44 [0] 207 951 9310

neds@uk.ey.com
www.ey.com/uk/independentdirectors

ERNST & YOUNG LLP

www.ey.com/uk/independentdirectors



In line with Ernst & Young's commitment to minimise its impact on the environment, this document has been printed on recycled paper.

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member practice of Ernst & Young Global.

Ernst & Young LLP, 1 More London Place, London SE1 2AF.

© 2008 Ernst & Young LLP. Published in the UK. All rights reserved.

3983.indd 01/2008 Produced by Ernst & Young Creative Services.