

# The Role of the Audit Committee in Risk Management

Paper prepared for the Audit Committee Chair Forum

by Dr Ruth Bender, Cranfield School of Management

The Audit Committee Chair Forum (ACCF) is convened by the CBI and Ernst & Young and is facilitated by Cranfield University.

The Forum comprises a select group of audit committee chairs from the UK's leading companies. Our aim is twofold, namely:

- to influence the direction of regulation as it impacts audit committees, and
- to act as a vehicle to develop points of view and best practice.

The Forum provides an opportunity to contribute to the debate, influence its direction and improve the performance of audit committees.

The Forum is currently chaired by John Buchanan, Audit Committee Chairman of AstraZeneca, with Gerald Russell, Senior Partner at Ernst & Young, and Martin Broughton, President of the CBI.

This is the sixth paper produced by the ACCF. Previous papers include:

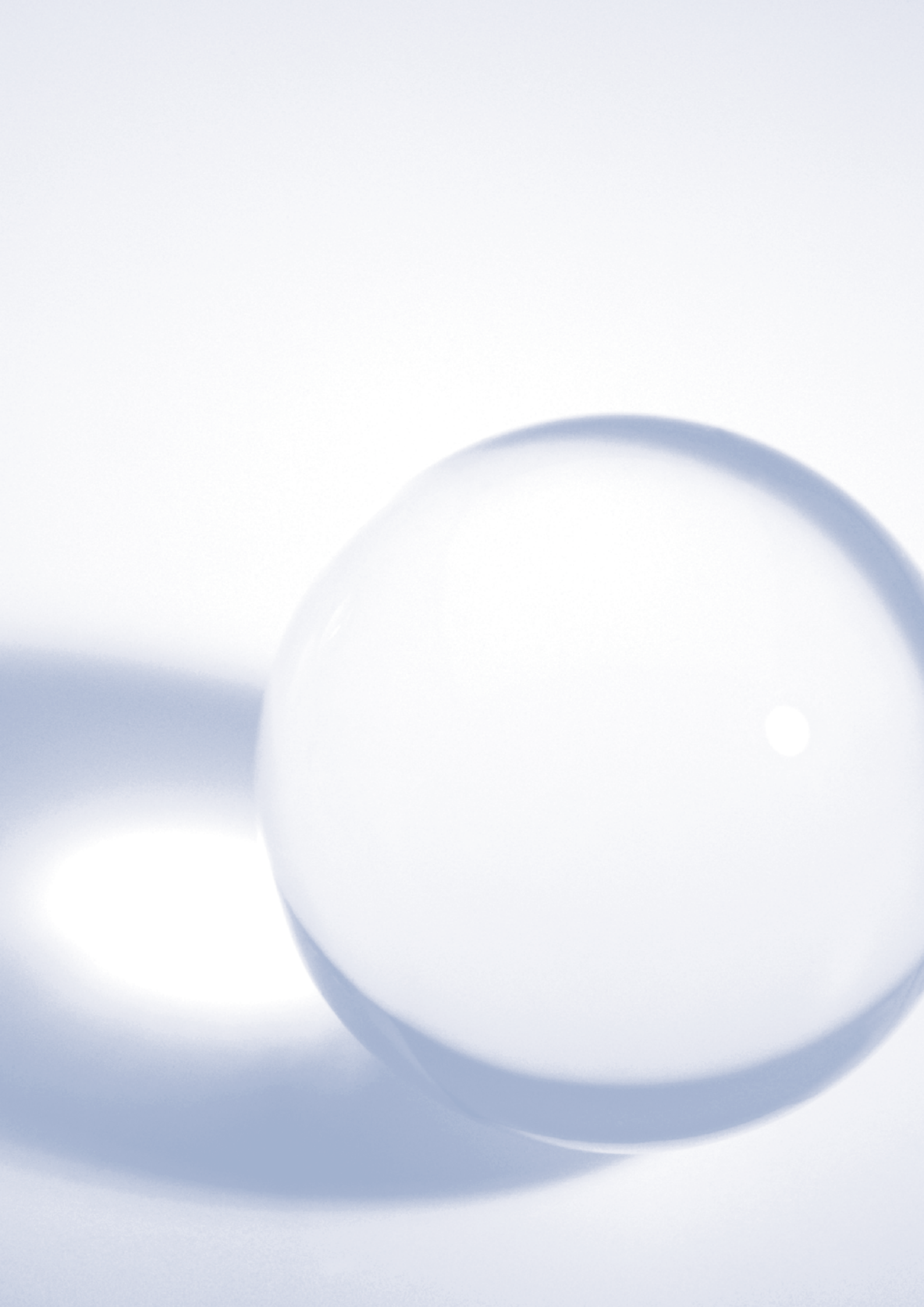
- What is an effective audit and how can you tell?
- The drivers of audit quality
- Audit Committee regulation: 'Financial literacy' – what does it mean?
- The role and function of the Audit Committee
- Audit Committee Communication: What is said, why, how and to whom?

*To obtain copies or learn more about the ACCF please contact the Forum Secretary, Gordon Cole at the CBI, [gordon.cole@cbi.org.uk](mailto:gordon.cole@cbi.org.uk)*



## Executive summary

- Risk is a Board responsibility, which cannot be delegated. The boundaries of the audit committee lie somewhere below strategic risk, which is a Board function, and above detailed internal control, which belongs to management. However, there was no consensus about just where those boundaries lie.
- The flipside of risk is opportunity, and the Board should set a risk appetite for the organisation that reflects this.
- The Combined Code suggests a role for a Board-level risk committee, comprising independent non executives. The participants in the discussion did not think this to be practical: risk management must involve executives.
- There is a danger that too much focus on the process of risk management could lead to complacency or to a lack of focus on the risks themselves.
- The review of risk at Board and audit committee level necessitates having non executive directors with a suitable range of backgrounds. The skills mix, as well as financial, should include high-level business knowledge, for example the understanding of significant opportunities/risks specific to the business.
- A key aspect of risk management is understanding the culture of the organisation. Non executives, with limited contact below Board level, may find difficulty in understanding the culture at lower levels of the organisation.
- The audit committee's role in risk management requires a strong relationship with the internal audit function of the organisation, one of whose roles is as a 'financial policeman'.
- Different types of risk should be addressed in different ways. Financial, operational and strategic risk have little in common, and their management and review should reflect the context of the particular company.



# Contents

Executive summary

---

Introduction 2

---

Opportunity - The Flipside of Risk 3

---

The Regulatory Background 4

Types of risk 4

The relationship between risk management and internal control 5

---

Structuring Risk Management 6

The role of the risk management committee 6

The role of the audit committee 7

The role of internal audit 9

Training and experience 10

---

Beyond Process 11

Identifying key risks 12

Evaluating risk management 13

---

A Final Thought 14

---

Questions to Ask Yourself? 15

---

Appendix 1 Questions included in the briefing paper  
supporting the meeting 16

---

Appendix 2 Internal control - Extracts from the revised  
Turnbull guidance 17

---



## Introduction

Understanding, monitoring and mitigating risks are fundamental tasks in successfully managing and running a company. They are also seen as a basic aspect of good governance. As such, Boards have to determine where all aspects of risk management lie, as between the full Board, its committees, and the executive management. Responsibilities have to be allocated regarding operational and strategic risk as well as financial risk, and processes should be in place to ensure that no key matters are overlooked.

Determining an appropriate risk management structure within a business and its governing Board is a vital task, and one on which practices differ. There is no right answer.

This paper reflects the discussions of a meeting of the Audit Committee Chair Forum (ACCF) held on 10th July 2007 to address the role of the audit committee in risk management. Additionally it draws upon telephone interviews with five members of the ACCF (two of whom attended the meeting); upon a selective review of relevant academic and professional literature; upon dialogue with professional risk managers from a range of organisations; and upon interviews and discussions previously conducted with members of the ACCF.

The interviews and meeting directly related to this matter solicited the views of ten Chairs of the audit committees of leading companies, four audit partners from Ernst & Young, and a representative of the CBI.

The paper sets out some of the issues relating to risk management at the top of the company. It does not consider the concerns faced by companies arising from the Sarbanes-Oxley Act in the USA, nor the specific risk requirements of businesses in regulated industries such as banking. Nor does it deal with the content or format of the Board's statement on internal control, required by Combined Code (2006): our focus is on the work undertaken rather than the reporting thereof.

The questions addressed in the briefing document circulated prior to the ACCF meeting, not all of which were addressed at the meeting, are set out in Appendix 1.

## Opportunity – The Flipside of Risk

*“We have a risk appetite – without that there is no profit.”*

A clear theme underlying the discussion on risks was the acknowledgement that risk-taking is an essential part of business, and without risk there is little opportunity to make a return. Risk management was considered in the light of the need for the Board to set a broad policy defining the company’s risk appetite, but with an appreciation that this has to include risk-taking ability. There was no desire to manage away all the risks faced by a business, but it was agreed that it was important to understand the risks being taken.

*“The focus is on the risks you are trying to avoid. But you should also look at the risks you are trying to take – that’s a Board decision.”*

### The Regulatory Background

The audit committee sits in a governance environment and within the UK the relevant regulation as regards its role in risk management is contained in the Combined Code (2006), which draws upon various underlying reports such as the Smith Guidance on audit committees (2003) and the revised guidance on internal control published by the Financial Reporting Council in 2005. Key matters are outlined in Table 1. *Overleaf*

Table 1 Outline of UK regulation concerning roles in risk management			
Source	Role of the board	Role of audit committee	Role of the executive (management)
Combined Code (2006) (Sections C2, C3)	The board should maintain a sound system of internal control.  It should conduct an annual review of the effectiveness of all internal controls, including financial, operational and compliance controls and risk management systems.	A main role of the audit committee is review of the company's internal financial controls and (unless there is a separate board risk committee of independent directors) its internal control and risk management systems.  The audit committee's role also includes monitoring internal audit.	N/A
FRC Guidance on Internal Control (2005) "revised Turnbull" (Paragraphs 15, 17, 25)	The board of directors is responsible for the company's system of internal control.  It should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning effectively.  The board must further ensure that the system of internal control is effective in managing those risks in the manner which it has approved.	The role of board committees, including the audit committee, is for the board to decide, and will be context-dependent.  Any work delegated to committees should be reported to the board.	It is the role of management to implement board policies on risk and control; to identify and evaluate risks for consideration by the board; and to design, operate and monitor a suitable system of internal control


The regulation summarised in Table 1 gives rise to considerations of the structure of risk review and management, and of the definitions of risk and internal control. Discussions of how risk review and management are addressed within companies were the main focus of the ACCF meeting, and are considered in detail in later sections of this report.

## Types of risk

*"There isn't a neat dividing line between financial risk and other risk."*

Implicit in the UK governance regulation on risk management is the fact that it should include non-financial risks. However, nowhere in the regulation is there a definition of the various types of risk faced, be they financial, operational, commercial, strategic or any other variety. The participants in these discussions used the terms 'financial' and 'non-financial' risk, but never defined them. The general understanding was that financial risks revolve around the integrity of financial systems and the risk of presenting misleading financial information. Treasury matters may also be considered as financial risk in some organisations.





Part of the difficulty in defining the role of the audit committee in risk management, vis-à-vis that of the Board or the executive, arises from the range of activities to consider. The practicality of lumping together operational and strategic risks as ‘non-financial’ was challenged. These risks have very different profiles, and combining, for example, a SWOT<sup>1</sup> analysis of strategic issues with a health and safety review could diminish the value of both.

Several participants mentioned that businesses generally appear to have better processes around the management of financial risk than other types of risk. There are various historic reasons for this, including the requirement for statutory audit and the fact that most internal auditors come from a financial background.

### **The relationship between risk management and internal control**

The regulation refers to risk management and to internal control. A very useful delineation of these concepts was given by one of the interviewees. He set out the overall process in three parts. First, one determines the risks that the particular company faces. This is followed by a decision as to how those risks are to be mitigated to an acceptable level. And internal control comes in at the third stage, to ensure that this risk assessment and mitigation is being done properly<sup>2</sup>.

Where each of these processes lies, between Board, audit committee, management and internal audit, differs between companies.

---

<sup>1</sup> Strengths, Weaknesses, Opportunities and Threats.

<sup>2</sup> This distinction mirrors that of the Turnbull report, set out in Appendix 2.

## Structuring Risk Management

*“The Board is somewhere between reviewing or assessing the big risks, not just strategic risks. Then the Board works through its committees. What is delegated down to the audit committee? ... Where are the boundaries?”*

*“Managing risks is part of the day-to-day role of the executive, and you can’t take it away from them.”*

As shown in Table 1, the Board is ultimately responsible for all aspects of control and risk management, not just financial controls. This has been the case since the original Turnbull guidance was published in 1999. Thus the Board should include non executives (NEDs) with sufficient knowledge to undertake such reviews. Whether or not these NEDs sit on the audit committee will depend on whether the risks are formally addressed by that committee, by a separate risk committee, or by the Board in full session.

It is also important to note that although “the buck stops at the Board”, to quote one of the participants, it was agreed by all that risk management should “live and breathe” at all levels throughout the organisation.

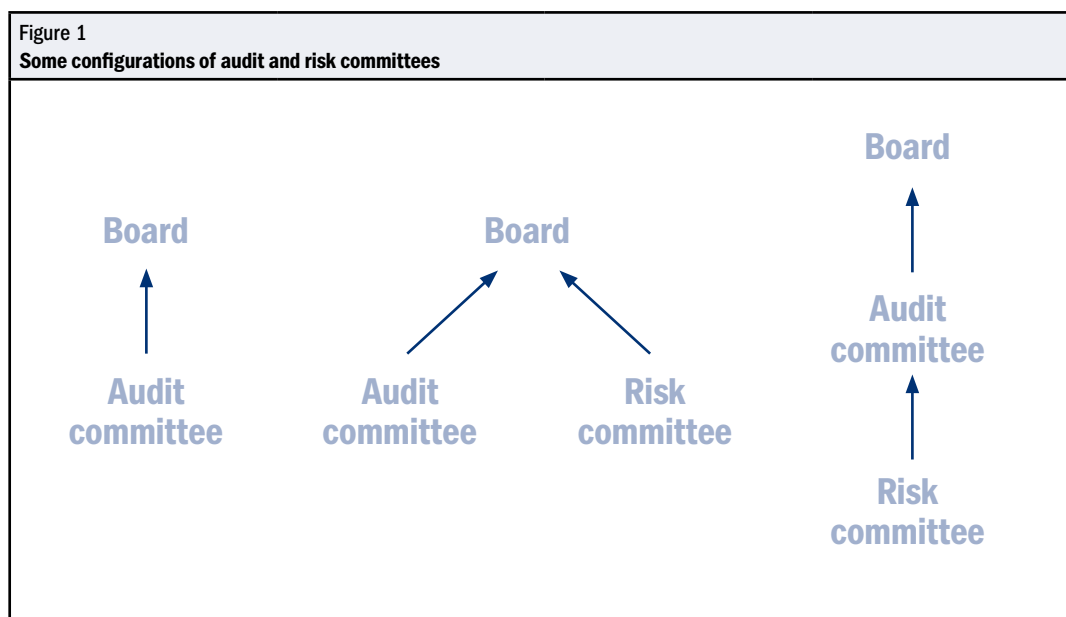
The following sections highlight some of the key elements in the discussion about where risk review and management lie.

### The role of the risk management committee

*“I can’t think of any circumstances where it’s appropriate to have a risk committee comprising only non executives.”*

*“If you have a risk committee and you have an audit committee, how do you know there aren’t any gaps?”*

Risk management structures differed, with separate risk committees, where they existed, reporting either directly to the Board, or reporting through the audit committee. Examples are shown in Figure 1.



In all cases where there was a separate risk committee it included executives; in most it comprised solely executives. This was seen as fundamental to its work, as the executives have a much closer understanding of the business, and the ability to manage the risk. Thus, practice differs from the position of the Combined Code, which suggests it would be possible to have a risk committee composed exclusively of NEDs.

*“If there is a risk committee, I don’t think that as a NED you can not be on that committee. ... And the risk committee shouldn’t just be NEDs, it should include execs. ... I part company from the Code on that one.”*

### The role of the audit committee

*“... [non-financial risk] is a Board thing and not an audit committee thing. The audit committee have to do it for the financials, but personally I don’t think we have the right skills around the audit committee; it’s too broad for the audit committee.”*

*“Audit committees need to avoid being too detailed. [You must] keep a focus. Otherwise it ends up being a surrogate Board.”*

Opinions at the ACCF meeting, and in the interviews that preceded it, differed markedly as to the audit committee’s role in non-financial risk. Whilst there was agreement that the ultimate responsibility lies with the Board as a whole, and that operational responsibility lies with management, the committee’s level of involvement was ambiguous.

Many of the audit committee Chairs took the view that risk management was a broad process, and the committee should consider all risks, much in the way implied by the Code and the Turnbull guidance. However, a substantial minority argued that the committee should have a much more narrow focus, concentrating on financial risk, and that general risk assessment clearly belonged at Board level.

At one end of a continuum of views, an audit committee Chair commented on how useful it had been to formalise the review of non-financial risks at audit committee, and how much benefit the organisation had obtained from this process. However, at the other extreme, a comment was made that this was just imposing a parallel management system on something that had been working well anyway, and there was no economic need for such. In this regard, it was suggested that risk management of operational items was just part of the day-to-day job of the line managers and their immediate superiors, and so there was little to be gained from imposing additional control and review systems. One interviewee argued that if, historically, no problems had surfaced, this in itself provided a level of confidence in the procedures adopted.

*“In practical terms the management of risk is the executive committee’s responsibility. ... For the big [risks], you’ll be comforted by the fact that these people have thought about it and written it down.”*

Of those whose audit committees did look at all types of risk, this was done in varying ways. In one company, the committee Chair stated that three major risks had been identified that were considered at every Board meeting, with the monitoring of all other risks delegated to the audit committee for its regular meetings. Another committee Chair commented that risk was considered formally in an annual process rather than at every meeting, unless something had changed. He also pointed out that risk review is “a biggish exercise” and that the first time through was the most interesting.

On a related issue, one of the participants in the discussion made the following point:

*“Audit committee is a compliance committee. Risk is not a compliance issue, it’s a Board issue. I don’t think that the Board should be delegating to a governance committee fundamental Board issues. The Board should delegate compliance to committees, and keep fundamentally business issues for the Board.”*

This definition of the audit committee as being solely ‘compliance’ did not meet with universal agreement, as some in the meeting saw its role as wider than this.



## The role of internal audit

*“Every audit committee I’ve been on spends a huge amount of time with the director of internal audit: for the year ahead, what is going to be audited, and what resource is available? ... It’s probably the only time with the non executives that you get detailed into the organisation. It’s the most ‘executive’ thing you get as a non executive.”*

As indicated by the above quote, internal audit tends to play a large part in the review of risks, both financial and non-financial. This is highlighted in the Institute of Internal Auditors’ definition of internal audit, set out below.

### **The official IIA definition of internal auditing**

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation’s operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

The responsibility to manage risk always resides with management. Internal audit’s role is to identify potential problem areas and recommend ways of improving risk management and internal control.

Internal audit may be provided by in-house staff, or an outsourced team. Either way, it is independent of the management structure, and reports directly to the audit committee. This independence gives it a unique and valuable perspective on risk management and internal control processes.

<http://www.iaa.org.uk/about/internalaudit/>

Over the past decade, the work of internal audit has changed. The original Turnbull report in 1999 significantly raised its profile by highlighting its role in internal control and risk management.<sup>3</sup> It expanded beyond the accounting function to include an operational review role, which is sometimes seen as more interesting and high-profile. However, in the light of the financial scandals in the USA, some companies appear to have taken internal audit back to its more traditional roots, with a focus on financial systems.

*“Internal audit are the FD’s Rottweilers. That’s how it should be.”*

The majority of internal auditors still have a financial background rather than, say, an engineering background. Thus, if their role is broadly-defined, it is important to ensure that their combined skills are appropriate for the work they are being asked to do, and they don’t stray outside their areas of competence. In practice, they often buy in the skills they need.

The internal audit department has a role to play in risk management, and it was agreed that the internal audit programme should coincide with the assessment of key risks. It appeared from the interviews that this was done more thoroughly by the audit committees in some companies than in others.

<sup>3</sup> See Page and Spira (2004). The Turnbull Report, Internal Control and Risk Management: The Developing Role of Internal Audit, Edinburgh: ICAS.

Best practice suggests that internal audit's reporting line be through the audit committee. A poll of those present at the ACCF meeting showed that their internal audit function reported to the finance director (FD) or the CEO on day-to-day matters, but always had a direct line to the audit committee when needed, and sometimes dotted line reporting to the Chair of the committee.

## Training and experience

*"If the audit committee comprises a lawyer, a politician and an academic, then you should fire the chairman!"*

*"People who are not attempting to train are probably running ... some risk"*

Regulation demands a certain level of financial literacy in at least one member of the audit committee. However, no such requirement is in place as regards their qualifications or experience in general risk management. Indeed, risk management is such a broad topic that it might be difficult to define what sort of expertise is needed.

It was agreed that it is up to the Chair of the company, possibly in consultation with the Chair of the audit committee, to ensure that the NEDs have sufficient expertise to staff the committee in its required responsibilities. None of the interviewees mentioned the need for any formal qualifications or risk management experience, nor for any such training; a broad business experience was considered sufficient.

At a previous meeting of the ACCF, members agreed that it would be inappropriate for regulation to insist on a high level of financial literacy for all audit committee members, as this might imply a narrow range of backgrounds and could limit the committee's ability to evaluate wider business matters<sup>4</sup>. Risk management would appear to be one example of where a variety of experience is an advantage.

---

<sup>4</sup> Audit Committee Regulation: 'Financial literacy' - what does it mean?, summarising the ACCF meeting held on 5th April 2006.

## Beyond Process

*“Having too much on the risk register runs the risk of diluting the focus on the key risks.”*

*“The challenge to us all is to make sure the executive are as engaged as they can be, and the management of risk is not just an annual box-ticking exercise.”*

A frequent criticism of corporate governance in general is that it can degenerate into a box-ticking exercise, not tailored to a company’s circumstances and with little original thought being applied. This accusation was also applied to the process of risk management, at Board and in the audit committee.

More than one of the participants in the discussions voiced strong opinions that risk management processes at this level were getting in the way of the business. It was pointed out by one that private equity companies manage their investments without the need for such formal processes. They focus on the key risks to the business model, and leave everything else to management. This echoed comments made in a telephone interview about how management were competent to do this without the need for much interference: *“that’s what they do for their day job”*.

Those participants who believed that the Board and committee did have an important role in risk management also emphasised the problems with a focus on ‘process’. When having to deal with the Combined Code, Sarbanes-Oxley and the introduction of International Financial Reporting Standards, it can sometimes be difficult to see the bigger picture.

In order to combat this, one of the Chairs had instituted a practice of creating ‘white space’ at his audit committee meetings; a period where there was no set agenda item, and the audit committee members could bring up issues for discussion on a wider basis. This was seen as being very useful.

Without this, things can be missed. Similarly, an emphasis on the process can lull audit committee members into a false sense of security, believing that because they have an extensive risk register, it means that all risks are being dealt with. As an illustration, one of the participants described a Board that had missed an important element of operational and strategic risk:

*“There’s a difference between understanding risk and hearing about risk – it’s the difference between successful businesses and businesses that go wrong. They [the Board] were getting lots of presentations. Because they were listening to it, they thought the controls were happening.”*

## Identifying key risks

*“I think it’s a good thing if the NEDs – Board or audit committee – sit down and ask themselves what they think the main risks are.”*

At Board level and, by extension, at audit committee level, what is important is to ensure that the key risks are identified, and that appropriate risk management processes are in place and are applied.

At the meeting, a discussion took place concerning company culture as a risk factor, and whether the NEDs were in a position to identify cultural problems that might imply that the stated codes and procedures were not being followed.

Two sets of views were aired. To some of the Chairs, “shoe leather management” was the way to understand the culture, and being seen around all of the business units would engender trust in them and enable them to find out more about the business and surface potentially damaging issues. However, others argued that in large organisation, NEDs could not possibly spend sufficient time doing this, and that inevitably they saw a sanitised version of the business.

One trend in governance that has in some ways distanced the NEDs from company culture is the growing tendency for Boards to contain fewer executive directors – often only the CEO and the FD. This can isolate the NEDs from other layers of the executive, let alone the people below them. Thus, particularly if there is a ‘command-and-control’ CEO, it was considered important for the NEDs to make the effort to reach further down the organisation.

*“We asked our partners, what is the main topic you discuss with your audit committees? It’s all around the quality of the people.” [Audit Partner]*

Leaving aside the cultural risks, another discussion took place about the appropriate level of involvement for a NED in appraising significant business risks. A fashion business was used as an illustration. A key risk in this type of business is that the buyers mis-read the coming fashions, and purchase the wrong merchandise. This is potentially serious, but such a risk is difficult for the unqualified NED to assess. It was agreed that this is why risk management needs to lie with the executives rather than the NEDs; the non executive role is to review. As one participant responded:

*“It’s not the role of the non executive to know whether you should have stripes or spots. It is the role to know what bets are being placed, and how big.”*



## Evaluating risk management

*Q “How do you know that risk management is being done properly?”*

*A “You don’t! How do you know the bank reconciliation is being done? You rely on processes, look at minutes, check that issues are being raised.”*

As already stated, risk management threads throughout the organisation. Risk registers are compiled by line managers, listing and evaluating the risks under their own areas of control, and these are recorded, assessed and then aggregated. Although the ultimate responsibility lies with the Board, the process cascades through the group. And in a multi-business group, this can mean that a wide variety of risks gets subsumed into some large, generic categories by the time the register reaches the audit committee or Board.

During the telephone interviews, participants were asked how they ensured that appropriate risk management was taking place, and how, given the fact that risk registers at group level inevitably hide a lot of detail, they were sure that they were seeing what they needed.

One Chair explained how he dealt with this. In order to overcome the generic feel of the risk register presented to the Board, he looked not just at the top ten or so risks, but at the top 30 – 50, and went through them in some detail with the head of internal audit. In this way he could appreciate how they had been prioritised. He looked at gross risk as well as net risk, so that he could understand the full potential, and also see if he was satisfied with the risk mitigation processes that had been put in place.

*“I think the audit committee’s role is to make sure that risk management is taking place. It’s to review the risk management process, to see the results of that process. And the most critical thing to me is to make sure that what comes out of the risk management process is reflected in, principally, the internal audit plan but also the external audit plan.”*

## A Final Thought

*“Risk analysis is just too important to be left to any committee.”*

*“The buck stops with the Board; the Board deals with this by delegation.”*

The Audit Committee Chair Forum is, by definition, a meeting place to discuss the practicalities of running audit committees. It was interesting that in this discussion, more so than any other in the series so far, participants made little distinction between their work on the committee and their work on the Board. Risk review (other than financial risk) was seen inescapably as a Board function, albeit in some companies one that is delegated in part to the audit committee.

*“I think it’s a shame that it’s called the ‘audit’ committee. If it were called the ‘committee to which this [assessment and monitoring of the systems of internal control and risk management] is delegated’ it would be so much more clear.”*



## Questions to Ask Yourself?

1. How does your Board set its risk appetite?
2. How do you ensure that all major risks are identified to and reviewed by the Board?
3. Are risk review and management allocated between the Board, the audit committee and the executive in the most appropriate way for the company's changing circumstances?
4. As a non executive, how can you ensure that all risks are being dealt with in the most appropriate way?
5. Is the board's annual assessment of the internal control structured, scheduled and able to engage the appropriate representation from the senior management team to allow an open dialogue on risk management and internal control arrangements?

# Appendix 1

## Questions included in the briefing paper supporting the meeting

1. As regards financial risks, what is the role of the Audit Committee vis-à-vis the Board, the Executive and Internal Audit? How does it carry out that role?
2. As regards the management of other risks, such as operational and strategic issues, what is the role of the Audit Committee vis-à-vis the Board and the Executive? How does it carry out that role? What training, qualifications or experience are appropriate for Audit Committee members dealing with a wide range of risks?
3. Is the Board over-delegating the risk management function to the Audit Committee?
4. What should be Internal Audit's role in respect of non-financial risks?
5. Under what circumstances is it appropriate to have a separate Risk committee that reports directly to the Board? How could you ensure that no significant risks are overlooked?

### Also:

Do Boards obtain the “regular assurance... that the system of internal control is functioning effectively” required by the FRC guidance? (See Table 1.) If so, how?





## Appendix 2

# Internal control – Extracts from the revised Turnbull guidance

### Para 1

A company's system of internal control has a key role in the management of risks that are significant to the fulfilment of its business objectives. A sound system of internal control contributes to safeguarding the shareholders' investment and the company's assets.

### Para 19

An internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together:

- facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud and ensuring that liabilities are identified and managed;
- help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organisation;
- help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business.



This document has been printed on recycled paper.