INDEPENDENT
AUDIT LIMITED

www.independentaudit.com
Holland House 4 Bury St.
London EC3A 5AW
T: +44 (0)20 7220 6580
F: +44 (0)20 7220 6581

Chris Hodge
Financial Reporting Council
Aldwych House
71-91 Aldwych
London WC2B 4HN

9 October 2009

Dear Chris

## Response to second consultation document July 2009

Independent Audit Limited is a specialist consultancy which amongst other things advises boards and their committees on the effectiveness of their corporate governance. Our clients include a wide range of companies, both large and small.

We have recently undertaken research on behalf of The ICAEW Foundation into risk governance in non-financial services companies. The resulting report is being published on 12 October. We hope that you will note that in the report we set out our views on the possible implications of the findings for the Code and these can be regarded as part of Independent Audit's submission to the Consultation. (Copies of the report "Getting it right" will be available at www.independentaudit.com/publications.)

### Comments on Section 1: Content of the Combined Code

We agree fully with the three guiding principles as set out by the FRC. Primarily this means avoiding increased prescription and encouragement of better disclosure to avoid boiler-plating and box-ticking.

We feel it would be undesirable to distinguish between BOFIs and other companies in the Code. The Code needs to continue to be principles-based, with companies being encouraged to work out what structures and processes work best for them. It would be unfortunate, therefore, if changes directed at BOFIs would come to be seen to be applicable to all companies and there is a distinct danger that this will happen by default. We would recommend, therefore, that if the Walker Review does result in some specific requirements or standards directed at BOFIs, that these be applied through a means other than the Code – or at the very least included as separate guidance appended to the Code and not included as specific provisions affecting all.

REGISTERED IN ENGLAND NUMBER 4373559
REGISTERED OFFICE: NARROW QUAY HOUSE,
NARROW QUAY, BRISTOL BS1 4AH

**The role of the board, chairman and NEDs**

Connected with this, we believe it would be helpful for the preamble or Principle A.1 of the Code to give much greater weight to the responsibility of each board to work out – and set out clearly – its role, the way governance functions in the business and how this relates to the work of the committees including the executive committee. In our experience, if this is not thought through fully and if there is a lack of a consistent understanding across the board and with management, board governance will not be fully effective. Boards should report explicitly on how they have confirmed their role and offer a full, non-boilerplate explanation in the annual report.

We agree with the emphasis to be placed on the chairman's role and that it would be helpful to include further clarification on what is to be expected from a chairman, the SID and non-executive directors, but think that this should be included as guidance not as provisions.

We do not believe it is helpful to be more specific about the time a NED should spend on their role. Minimum time commitment is less important than how that time is spent. NEDs should spend time in the business as a means of gathering insight and understanding. The efficiency of individual NEDs is very dependent on the efforts made by the management to provide information and support, and there is no direct correlation between time spent and individual effectiveness. We think it would be positively unhelpful to encourage boards and others in the belief that the quality of corporate governance is in any way related to how much of it there is.

We therefore think that a more useful recommendation would relate to what is expected of NEDs and the obligation on management to provide user-friendly information, transparent process and practical support to enable the NEDs to be effective. The amount of time necessary to achieve this can be left to individual boards; if they choose to invest for the purpose of increasing the efficiency of NED oversight, they should be allowed to reap the benefits.

**Board balance and composition**

The need for a suitable mix of expertise and experience in a board, and not only those of banks, is a very important point which should be emphasised. Training, support and time are relevant to equipping NEDs to contribute to good risk governance, but other characteristics such as the experience and qualities of individual directors and the balance of the board in relation to its strategy and the risks it is taking are even more vital. These points could be emphasised more fully in the Code.

We agree that the way the independence criteria have been applied by some boards or interpreted by many investors is unhelpful. It may well be the case that a NED needs several years to build a good understanding of the business. As a result the benefits of longevity of tenure that come from this knowledge and experience may outweigh any downsides relating to independence (and we in any event seriously question whether independence is related strongly to tenure). We recommend that consideration be given to removing from the Code references to specific tenure periods in the context of independence while keeping references to the timing of directors being put forward for re-election (see below).

We feel that the "minimum 50%" requirement is probably unhelpful. In numerous cases it appears to have led to reductions in the number of executive directors in order to prevent the board becoming undesirably large. The key question is the role the NEDs play and how they behave, not the absolute number. Again it comes back to the role of the board and the company providing an explanation of how it works, its governance goals and how the structure of its board supports achievement of those goals.

We agree that more emphasis should be placed on succession planning. This should be through a combination of a requirement for improved reporting on the board's approach to long-term succession planning and a more explicit requirement for an evaluation of the nomination committee's work and the board's approach to succession planning.

**Frequency of director re-election**

We do not agree that the chairman of the board or of the main board committees should be proposed for election annually. We think that the potential benefits of this are on balance outweighed by the risk of instability and of discouraging candidates. A possible alternative would be for the normal three-year terms for the chairman, SID and audit and/or risk committee chairman to be staggered so that one was up for re-election each year. This would give shareholders the opportunity to vote on a significant board appointment every year.

Also we do not agree that all directors should be put up for annual re-election. This would introduce too much instability and possibly the opportunities for "gaming" that you refer to. Also, it implies that shareholders would have enough information to judge whether individual directors are performing well – it is difficult to see how this would be the case.

What is more important is to help increase investor confidence that the board is effective. This implies a combination of stronger board evaluation (see below) and better reporting on how the board operates. An advisory vote on the corporate governance report may help focus minds on these matters. It is an idea worth investigating further as it would focus the board's mind on how its governance is working in practice and on what they are saying they actually do. But it would be fraught with difficulty: what matters in practice is how the board behaves, not what it says it does and this is not something that can be fully ascertained from a written report. Any such votes would inevitably be based on impressions and we are not convinced that this would be a sound basis for a vote, even if it is only advisory.

**Board information, development and support**

We do not believe that the inclusion in the Code of more guidance on information, training and support would be helpful.

Boards and management need to work out between themselves the best structure for board information. There is no "one size fits all" and this area is too complex for Code-based guidance.

We agree that director attitudes to development (ie training, as everybody else is prepared to call it) are often disappointing and there is no doubt scope for boards to take this question more seriously, whether it be related to technical training or more general "being effective training" (eg through better use of case studies and scenario discussion).

We do not feel there would be benefit in recommending the development of a separate source of support for boards. If the relationship between the board and management is working well and the secretariat is properly staffed and effective, there should be no need for this. If it is not, there is a bigger problem and no level of dedicated support will help ensure that NEDs are better informed.

So it is difficult to see how "good practice" in these areas can be spelt out in Code guidance. What would be more beneficial in encouraging good practice would be for the Code to require more effective board evaluations which cover these issues and fuller reporting on how a board is going about making sure that continuous development of information and skills is addressed seriously by both the company and individual directors.

**Board evaluation**

While being strongly in favour of external evaluation (naturally, as this is what we do as a company), we are reluctant to suggest that it should become obligatory.

We believe an external review can be much more thorough (if done properly) and has the benefits of an independent view and fresh insights. But the timing of such reviews is a sensitive issue (eg due to board changes, mergers etc) and it would be unfortunate if investors started to criticise companies if they failed to keep to a requirement for eg an external review every three years. It may be preferable to introduce a requirement for companies to explain why they have opted for an internal review (self-assessment). Investors can then judge whether they feel the explanation is sound and valid – and see whether the same reason is given from year to year.

We agree that the requirement for all committees to be evaluated each year should be changed. In practice, most reviews of committees have proved to be superficial. It would be much more useful if the requirement were for an in-depth and standalone review of each committee to be conducted periodically, possibly every two or three years. Again, there should be full reporting on the approach, a description of the main findings, and an explanation as to why the board has opted for self-assessment if it has opted not to conduct an external review.

We feel it would be useful for individual assessments to continue to be annual. Individual performance can change during the year (possibly in response to previous reviews or changes in personal circumstances or commitments) and new directors join. Also, given that management and staff are subject to annual review, it would seem appropriate that directors follow a similar approach. However, we point out that, ultimately, individual director review is something that a chairman should be conducting and acting on continually.

We feel there may be some merit in a requirement for an "assurance statement" but that this should not aim to provide assurance that "the board is effective". Instead it should aim to cover, for example:

- The approach taken to review, including a justification of a self-assessment approach
- An explanation as to the main areas of focus
- A discussion of how the board has managed to avoid the "pitfalls" that boards and committees often fall into
- A description of how the board ensures that key issues around effectiveness (eg information, time, management relationship) have been reviewed.

This sort of statement could be useful but will be complex to put together as guidance. Also it will be important that such a statement does not become a "checklist" or boilerplate in nature. It may be that a "model statement "would be the most effective form of guidance. Independent Audit would be pleased to help the FRC with further, more detailed suggestions.

**Risk management and internal control**

Our comments in this area are extensive and we would refer you to the aforementioned report published by The ICAEW Foundation. (Note, however, that the suggestions made below are solely those of Independent Audit and not of The ICAEW Foundation.) Many are points that would be better captured in guidance than in the Code itself, but we have not attempted to second-guess how it would be best to incorporate any changes other than in some specific places where we have referred to Principles or Provisions.

Our detailed points are attached as an appendix to this letter. We make the following general suggestions that should be considered as possible changes to the Code or related guidance:

- Build into the Code preamble and A.1 a much clearer and greater emphasis on the board defining its role and how this relates to the executive team's responsibilities – including a specific reference to the board's responsibility for risk-taking, its role in risk oversight and the extent of its involvement in risk management.

- Give clear guidance on the role of the board and board committees in risk oversight and risk acceptance (A.1 or C.2?).

- Restructure Turnbull along the lines of the Smith Guidance so that the different elements can be readily identified, considered and assessed.

- While keeping the existing Turnbull content largely untouched, reduce the overwhelming focus in Turnbull on the process, checking of the process and reporting by addressing the striking lack of guidance on the behavioural aspects.

- Strengthen the Turnbull reference in the Code Principle C.2 by inserting a new provision that "Boards should consider how far their internal control and risk management are in line with the Turnbull guidance and what steps may be needed or beneficial to bring them further into line". (And possibly the same for the Smith guidance reference in C.3?).

- Expand the Provisions in C.2 along the lines of the audit committee (C.3) in order to cover the points listed below.

- Insert a section in the Code on what can/should be expected of the Chairman and NEDs in relation to board management of the risk process and board-level risk acceptance.

- Encourage boards to undertake a more active and structured approach to assessing the control culture and ethical environment. This may require a more formal review periodically.

Boards should be encouraged to report more openly on their approach to risk management, internal control and assurance. Most reports currently provide little useful insight and are boilerplate in style.

We do not feel it would be appropriate for all companies to be encouraged to have a separate risk committee separate from the audit committee with responsibility for oversight and advice to the board on the current risk exposures of the entity and future risk strategy. In our experience, and borne out by our recent work on risk governance in corporates, structures and processes do not of themselves result in good behaviour – motivations are too complex and people too good at working around process, whether with bad or with good intentions. Structures and processes are valuable insofar as they facilitate good behaviour, but it is rarely if ever the case that this can only be achieved by a particular structural or process solution.

It is how directors spend their time that matters most, not the committee structure in which they spend it. It is not proven that the existence of a separate risk committee leads to better governance of risk, and requiring such a committee is potentially misleading since it implies otherwise. We think that the recommendations should instead emphasise the responsibility of the board, and the need for it to ensure that it has the structures and processes in place to maximise the effectiveness and efficiency of its work.

The duties of a board in relation to risk governance include both making strategic decisions regarding the acceptance, rejection and mitigation of risk and oversight of the risk management processes. In the course of our professional work with boards we have observed that the former of these is already an area of potential confusion, and that the responsibility for establishing risk appetite is sometimes unclear. We think this is too fundamental to a director's duties to be delegated and that it should remain the clear responsibility of the whole board, with all directors having equal opportunity, and obligation, to participate. Many boards may wish to use a sub-committee to undertake detailed work in advance of consideration by the whole board, but mandating such a committee risks distracting attention from and undermining the whole-board responsibility.

In relation to the delegation of the work involved in risk governance, particularly the oversight of risk management processes, we again think that the case for separate risk committees is not proven. In our experience, the choice of structure involves making a trade-off which is dependent on a board's individual circumstances and the characteristics of the risks that have to be overseen.

A combined audit and risk committee is in principle well-placed to cover the whole range of issues without any risk of things falling down the gap between two committees. However, in large and complex companies (perhaps especially in financial institutions), or perhaps more precisely companies with a lot of complex risks, this can make the agenda too long to be manageable for the audit committee, and in practice the quality of oversight can sometimes be improved by having separate committees. We therefore think that whether to have a separate risk committee or a combined audit and risk committee is a decision that should be taken on practical grounds by each board.

### Remuneration

There should be a reference in the Code concerning culture and values, the board's responsibility for understanding how tone at the top translates into these, and the importance of non-financial incentives such as securing higher status.

The Code could usefully refer to the importance of board committees working with each other in the area of remuneration, for example, the remuneration committee receiving advice from the audit committee, and possibly assurance from the internal or external auditors, on the definition of and appropriate adjustments to performance measures. It should also highlight the importance of the remuneration committee liaising with the audit and risk committees to ensure that behavioural risks arising from incentive schemes are properly considered.

The effectiveness of a remuneration committee is very dependent on the competence of its chairman and members, which cannot be taken for granted in relation to complex reward schemes. There is room for the Code to address this topic. It should seek to ensure that committee members as well as the chairman have sufficient expertise to contribute. Our comments above on the need for in-depth effectiveness reviews of board committees apply particularly to the remuneration committee. Also there should be a requirement for a specific report from the remuneration committee on how it has met its responsibilities (in the same way that an audit committee has to report): currently this usually gets conflated with the remuneration report which has a different purpose, resulting in little insight into the work or effectiveness of the committee.

We do not believe that shareholders should be given a more direct role in setting remuneration: this is a task for the board and management to undertake on behalf of shareholders.

## SECTION 2: THE IMPLEMENTATION OF THE CODE

### Disclosure and enforcement

We do not feel that there would be much to be gained from switching from "comply or explain" to "apply or explain". The difference is one of nuance which is unlikely to have an impact on investor approaches. "Comply or explain" is a well-recognised expression that has entered common usage and is well understood, even if some investors then choose to ignore its intent.

We agree that, ultimately, responsibility for the effectiveness of "comply or explain" lies with companies and investors. The FRC could possibly play a limited role in promoting improved reporting on areas of "non-compliance" and better investor understanding of the "comply or explain" concept. But, ultimately, what is more important than "comply or explain" is the way companies explain the role of the different parts of their governance framework, how their governance works in practice and how it meets their needs. Putting too much emphasis on "comply or explain" can lead to a tendency to starting checking lists whereas it is the substance of what a company does that matters, not the form.

There would be merit is setting out what needs to be covered in corporate governance reports. This could include rationalisation of what needs to be reported and bringing together the references to reporting rather than having them dotted about the Code.

Also we feel that the FRC could provide more guidance on what should be covered in a governance report. But this should be in the form of guidance on the sort of issues that might be addressed and why they are relevant, rather than a list of required disclosures that could too easily become a checklist prone to boilerplate. Some model reports might be helpful.

We do not believe that the FRC can play a stronger enforcement role in relation to "comply or explain" statements. Ultimately, a company will report more effectively if it recognises the benefit in doing so – and in the absence of active interest from investors in governance communications there is little incentive for them to improve reporting. Monitoring by the FRC of non-compliance with the explanation requirement will achieve little.

Yours sincerely

Richard Sheath
E-mail: richard.sheath@independentaudit.com

**APPENDIX:**

**Specific points relating to risk governance that should be considered as possible changes to the Code or related guidance**

| | |
|---|---|
| **Applicability** | ***Structures and processes need to be suited to each business – "horses for courses"*** In the preamble state that certain structures and processes related to internal control and risk management that may be applicable to financial institutions, may not be equally applicable to non-financial services companies. Each board should consider the merits and decide on a structure that is best suited to their particular company. |
| **Role** | ***The board's "risk role" needs to be clear; consider it as "risk oversight" and "board-level risk acceptance"*** The board should ensure clarity over its role in risk oversight, considering the different aspects of (i) "risk oversight" of the risk management process and (ii) "board-level risk acceptance", setting out the extent of the board's role in identifying, assessing and accepting risk and its limits in relation to monitoring and mitigation (which primarily is a management responsibility). (Code Preamble, C2 and Turnbull 15) |
| | ***The respective responsibilities of the board and its committees need to be clear*** The board should be clear over the respective responsibilities of the board and board committees for risk oversight and board-level risk acceptance – and communicate this internally and externally so that the board can be held accountable. Boards should determine whether a board risk committee is required on a company-specific basis, taking into account their particular needs. |
| **Board structure** | ***The extent of the audit committee's role needs to be clarified along with the extent of delegation of "board-level risk acceptance"*** While the allocation of responsibilities between the board and the board committees should be company-specific, the board should (i) give detailed consideration to the role to be played by the audit committee given that its responsibility for financial reporting controls and internal audit effectiveness means that it must play a significant role in risk oversight whatever the adopted structure; and (ii) consider how far responsibility for board-level risk acceptance should be delegated to a board committee if not all directors attend the committee – or what reporting procedures will be put in place to ensure that all directors are involved in board-level risk acceptance. |
| | ***All directors must be involved in key risk acceptance discussions in a timely way*** Whatever structure is adopted, all directors must be involved in key risk acceptance discussions and decisions on a timely basis, especially in relation to merger & acquisition decisions. |

***Board committees must report effectively to the full board***
There should be effective reporting on risk oversight from the audit committee (or other responsible committee) to the full board in cases where some members of the board do not attend the relevant committee meeting.

**Leadership**

***The CEO must take the lead in supporting good risk management***
The CEO and other senior executives must be visibly committed to supporting good risk management practice, internal audit and other parts of the control and assurance structure. Consideration should be given as to how this is reflected in the CEO's internal and external messages.

***The Chairman needs to show leadership too and make sure the CEO does as well***
The board Chairman has an important role to play in providing leadership to the board on risk management issues and in encouraging the CEO to show the necessary executive leadership in maintaining a strong risk culture and risk management processes.

***The board must set the tone – and the audit committee take a lead***
The board as a whole, as well as individual directors, should play an active role in setting the right tone around control and risk through appropriate behaviour and consistent messaging. While not all parts of the board will be equally visible to the organisation, the audit committee does have a visible role to play in setting the control tone.

Walker Recommendation 9 (chairman's role in facilitating NED contribution) could be included to emphasise this in relation to risk.

**Culture**

***The target risk culture should be defined - and the board should assess how far it has been secured***
The board should debate and have a clear understanding of the risk culture it wishes to operate in the organisation and of its strategic and commercial relevance. It should formulate an approach to assessing periodically how far its target culture is prevailing on a consistent basis throughout the organisation.

***Openness and transparency need to be fostered***
Management and the board should demonstrate clear awareness of the need to foster an open culture which allows and encourages people to identify problems, weaknesses and the cause of failures so that lessons can be learnt and actions taken. Concealment should not be tolerated.

**Accountability**

***Manager responsibility and ownership need to be identified with accountability reinforced by information and audit***
Boards should ensure that manager responsibility for risks and risk mitigation is identified so that individuals can be held accountable through clarity of ownership, reporting lines and authority limits. The board should also ensure that such accountability approaches are reinforced by good information systems and internal audit. Consideration should be given to the role that can be played by self-certification and sign-off. (Turnbull 18)

| | |
|---|---|
| **Learning** | ***Major failures should lead to structured learning and boards should be involved***<br>A board should ensure that, in the event of a major failure, a structured approach to extracting and acting on the lessons to be learnt is adopted. In critical cases this should include detailed review by a board committee. (Turnbull 32) |
| **Risk appetite** | ***Boards should communicate their attitude to risk and risk tolerances through their strategic planning and on-going decisions***<br>Boards should communicate explicitly and effectively their attitude to risk, explaining clearly the levels and types of risk that are considered tolerable in strategic terms. This is likely to emerge from both strategic planning discussions and more regular consideration of risk positions and evaluation of risk as part of the board's decision-making. |
| **Reward** | ***Remuneration committees need to look at how reward systems generate risk***<br>Remuneration committees should consider the risk implications of remuneration systems adopted for senior executives and also those applying more widely across the organisation, assessing how the systems may increase risk-taking to levels outside the organisation's risk tolerance or have an adverse impact on the risk and control culture. (B.1; relates to Walker Recommendation 28) |
| **Scenario debate** | ***Boards needs to assess organisational resilience in abnormal situations***<br>Strategic review by boards should consider the organisation's likely resilience in the event of scenarios outside the norm. This may include periodic financial stress-testing and consideration of scenarios in which multiple risks crystalise simultaneously or extreme, improbable situations develop. |
| **Management structures** | ***The thinking behind risk management and assurance structures needs to be clear to the board***<br>Boards should have a clear understanding of management thinking behind the chosen risk management and assurance structures including the question of the location of the risk management function and the possible allocation of lead responsibility to a chief risk officer or to another senior manager or auditor. Whichever structure is adopted, the board must ensure that the responsible officer is of sufficient stature and has regular contact with the board.<br><br>***Risk management should be an integral part of business processes***<br>Risk management should be an integral part of business processes with operational management taking responsibility for identifying, assessing and reporting on risk positions and following risk acceptance policies. Reviews of the effectiveness of internal control should assess the extent to which this is the case. (C.2 and Turnbull Section 5?) |

***Risk management functions should play a facilitation role***
Although it will vary between organisations and a different approach may be required in financial institutions, corporate risk management structures are most likely to be effective when primarily playing a facilitation role. This helps ensure that risk management responsibility remains with operating units and continues to be an integral part of operating processes and decision-making.

**Information**

***Particular attention should be paid to "net" (residual) risk positions***
When reviewing risk reports boards should pay particular attention to changes in risks and "net" (residual) risk positions. In addition, the context within which the reduction to a "net" position has taken place eg the control environment and related assurance activity. The larger the reduction on a material risk, the more the attention that should be paid to it both in terms of controls and its position within the risk-based internal assurance framework.

***Risk identification should be an opportunity to review what's happening in the business – not just a process***
Periodic risk workshops and the regular formulation of "risk maps" should be seen as an opportunity to form a view on what is happening in the business rather than as part of a risk management process. Approaches to workshops should be regularly refreshed in order to avoid staleness and to retain management commitment.

**Assurance**

***Internal audit is a vital part of good risk management and must be supported***
Internal audit act as an important source of assurance for boards over risk identification and management, increasingly across the full risk spectrum. Boards should ensure that internal audit is adequately resourced to meet this need or ensure that other sources of comfort perform a similarly independent function. Visible and active CEO support for internal audit is vital.

***Risk-based auditing should be based on an integrated, corporate-wide view of risk***
Risk-based auditing is likely to be the most effective approach to audit planning and resource allocation. The responsible board committee should ensure that there is, as a minimum, close liaison between internal audit and any other risk management function to ensure a coherent and common view of the organisation's risk profile.

***An independent review of assurance and risk management is needed from time to time***
Given the importance of internal audit in ensuring that risk is well-managed and controls are effective, the board should consider conducting periodically an independent review of the effectiveness of the internal audit, risk management and other assurance functions.

**Evaluations**

***Board reviews should include a specific focus on the board's risk role***
The annual reviews of board and board committee effectiveness should include a specific focus on the board's work on risk oversight and board-level

risk acceptance. (A.6; relates to Walker Recommendations 12 & 13)

***The board's Turnbull review should include looking at the board's risk role and activity***
The board's annual review of internal controls should cover the approach taken to applying the principles and provisions set out in C.2 of the Combined Code and also the Turnbull guidance.

***Reviews should consider explicitly the risk and control culture***
In reviewing the effectiveness of internal controls the board should consider the risk and control culture of the business and how far this is embedded in a consistent way across the organisation. (Turnbull 24)

**NED engagement**

***NED engagement with management and other staff across the business through visits is vital for effective risk oversight***
To form a sound and encompassing view of risk and the organisation's attitude to risk and risk management, NEDs need to engage with management throughout the business – and possibly at other levels too. Regular informal site visits are likely to be an effective way for forming this view. This may take the form of solo visits as well as board visits. Full board visits also help by being an opportunity for the directors to get to know one another better. (C.2 )

***The board needs to have exposure to the wider executive team***
Board engagement with management at board and board committee meetings provides a board with valuable opportunities to judge attitudes to risk and risk management and so act as a further source of comfort. Opportunities to meet the wider management team should be sought on a regular basis.

***A more positive attitude to NED training on risk issues is needed***
Walker Recommendation 1 (business awareness/induction/training) and Recommendation 4 (NED qualities) bear expansion in the Code.

**Board composition**

***In securing the right board mix, the way skills and experience have a direct impact on the board's risk role needs to be explicitly considered***
In determining the right board composition and recruiting to secure it, specific consideration should be given to what type of experience will be needed to ensure the board can be effective in relation to risk and the necessary diversity. The mix of non-executives will need to be one which puts the board in a position to judge the key risks facing the business and help management in making risk judgements, as well as to consider the effectiveness of the management' approach to mitigating the risks. The board committee responsible for risk oversight also needs to include the right mix; this may mean ensuring that the audit committee is not overly dominated by financial expertise. (A.4?)

***NEDs need to be confident in challenging and speaking up on risk issues***
Particularly in relation to challenging management on the risks being taken and how they are being managed, non-executives need to be confident in speaking up and disagreeing when necessary.

***The benefits of understanding the business and risk that come from long service need to be balanced against any independence issues in considering tenure***

Building the knowledge of the business that provides a firm basis for challenge is often acquired over a number of years in a board role. In considering the length of tenure of a non-executive director, the board should take into account, and balance against the question of independence, the consideration that long-serving directors can bring particular knowledge and confidence to their role which can strengthen challenge, oversight and judgement of risks. Investors should also factor this in forming a view on the length of tenure of individual directors.

**External reporting**

***Boards should report on how they interpret and act on their risk-related responsibilities***

Reporting on how the board is meeting its obligations should include a description of how it defines the responsibilities of the board and its committees in relation to risk acceptance and oversight and how this responsibility has been exercised during the year. Explicit reference should be made to how the board's role in risk oversight and management differs from that of the executive team. (C2.1; A1.1; Schedule C)

***The report on internal control should give insight into how risk oversight and management operate***

The board's annual report on its assessment of internal control and risk management should aim to provide insight into how risk management in the organisation is structured to help it achieve its strategic objectives and maintain risk levels within agreed risk tolerances. This should include discussion of how the board and management determine that an appropriate ethical, risk and control culture is maintained consistently throughout the business. (Turnbull 32; relates to Walker Recommendation 27)

***The report should explain how the board has reviewed internal control***

The board should report to shareholders that they [have reviewed the effectiveness of internal controls] and explain how they have done this. (C.2.1; Turnbull 8)