Catherine Woods
Financial Reporting Council
Fifth Floor
Aldwych House
71-91 Aldwych
London WC2B 4HN

11 December 2013

Dear Catherine Woods

Consultation on Draft Guidance to the Directors of Companies applying the UK Corporate Governance Code and associated changes to the Code

Before addressing the specific questions in the consultation document, I would like to make some general comments.

Guidance or standard?

1. The draft guidance (paragraph 3) notes that recent high profile failures of risk management have emphasised to boards the need for properly considering risk. Arguably more companies have failed through ignorance of their risks than have failed through incorrect accounting, yet accounting is surrounded by detailed standards and risk only has a code plus guidance notes. I agree with this approach but believe that the linking of risk reporting with accounting, through the connection with *going concern* means that the guidance must use clearly defined terms and be free of ambiguity.

2. The Financial Reporting Review Panel Annual report 2012 noted

   - *Some companies continued to provide a list of bullet point headings rather than a clear description of the principal risks they faced.*
   - *Others did not clearly separate the company's principal risks and uncertainties providing instead a long list of potential risks. The Panel questioned the companies concerned as to whether all the risks and uncertainties in a long list were, in fact, principal.*

   However, the nearest the guidance comes to in a defining a *principal risk* is in paragraph 26 and the first sentence of appendix B, when it is applied only to solvency and liquidity risks. The definitions differ and appendix B uses the phrase *severe distress,* which is not one generally recognised within risk management. It seems rather harsh to criticise directors for failing to clearly identify principal risks and then not providing them with the clear guidance to do it.

Terminology

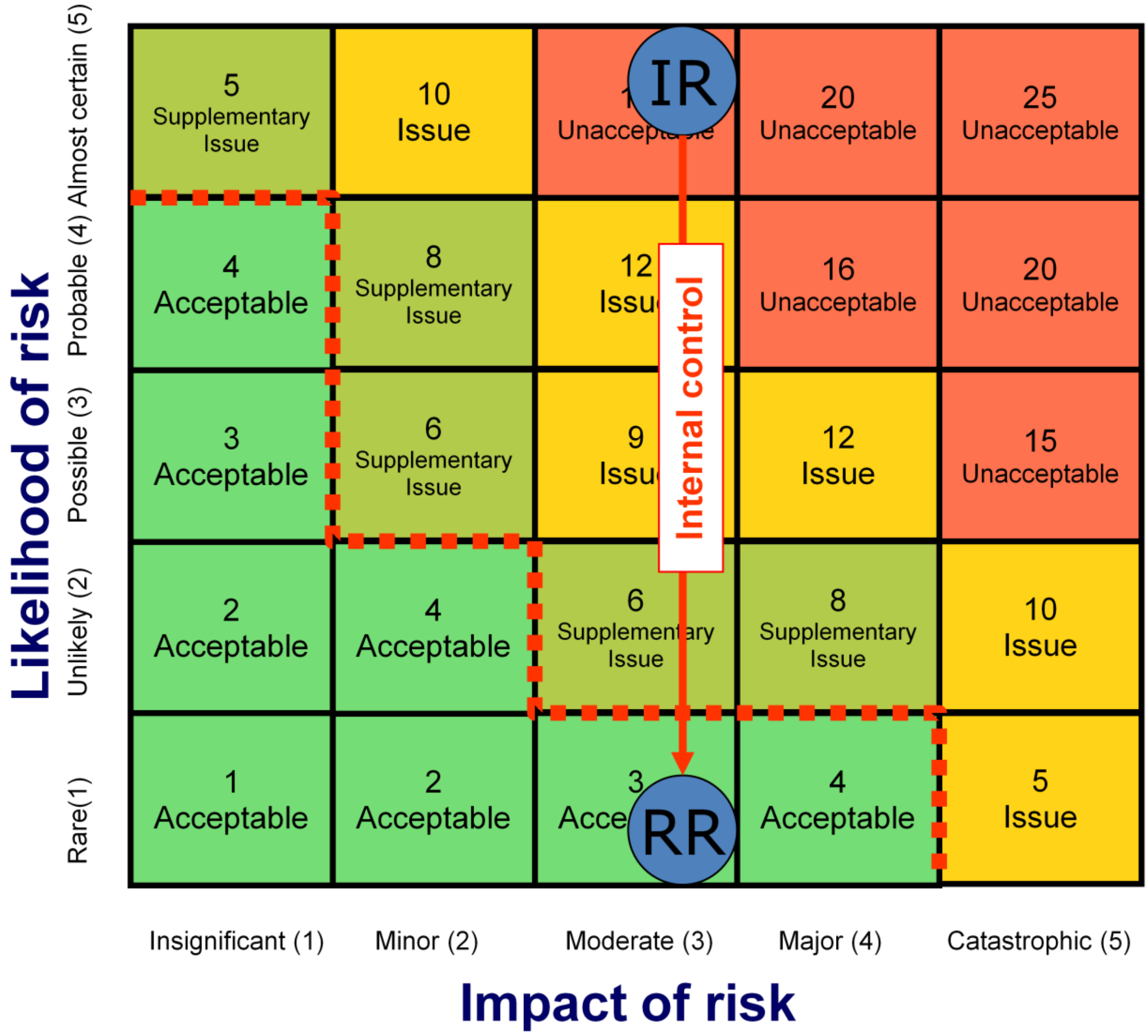
3. I therefore believe that the guidance notes require an improved definition of the terms used, explanations as to how some are linked and removal of some ambiguities. I will go into detail later but two examples are:

   Para. 19, first bullet point, notes the need for the board to determine its risk appetite but there is no mention of the link between this and the likelihood and impact of risks (para. 25).

   Para. 19, fourth bullet point, notes that risks should be controlled, managed or mitigated. ***Para. 26*** notes the principal risks should be avoided, transferred, mitigated or tolerated. In neither case is there any further explanation as to the meaning of these terms. In practice, *controlled* and *mitigated* usually mean the same: the application of internal controls. *Managed* refers to the four methods of dealing with risks mentioned in para. 26 (although the phrase *response to risks* is usually used to refer to these methods). Thus there is not only inconsistency between paragraphs 19 and 26 but the phrase *risk management and internal control* is tautology since internal control is a subset of risk management.

I am raising this point because I believe there is a need to define certain terms at the outset, either in the introduction or in the first appendix. My argument is that if it is desirable to include five pages of guidance in appendices B and C covering solvency and liquidity risks and the going concern basis of accounting, then it should be desirable to have two pages of guidance on the fundamental principles of risk management. This guidance could be provided by the generally accepted *risk heat map* show on page 3.

This map splits the parameters of risk (impact and likelihood) into the five divisions shown in the table on page 4 and shows the resultant 25 combinations on a graph. Each combination is then assessed as to the response required. Those combinations which do not require a response are considered to be below the company's *risk appetite*.



Unacceptable: Immediate action required to manage the risk

Issue: Action required to manage the risk

Supplementary issue: Action is advisable if resources are available

Acceptable: No action required

Risk appetite, as defined by the board

IR = Inherent Risk	RR = Residual Risk

The relationship of the heat map to the code and guidance is as follows (*para*. refers to paragraphs in the guidance where the terms are used):

- The generally accepted parameters used to measure risk (*impact* and *likelihood*) are shown as the two axes of the map (para. 5 and para. 25).
- The map demonstrates how a scoring system might be applied to *impact* and *likelihood*. The table on page 4 shows how the scores can be assessed. (Appendix C: Determining whether there are material uncertainties (a) refers to *impact* and *likelihood*)

If the impact when the risk occurs is:		The likelihood of the risk occurring is:		Score
To close down the organisation, or a significant part, for a very long period	O R	Almost certain	Then the measure is defined to be	Very high (5)
To prevent the organisation achieving a major part of its objectives for a long period		Probable		High (4)
To stop the organisation achieving its some of its objectives for a limited period		Possible		Medium (3)
To cause inconvenience but not affecting the achievement of significant objectives		Unlikely		Low (2)
To cause very minor inconvenience, not affecting the achievement of objectives		Rare		Very Low (1)

- The board will determine the combination of impact and likelihood it is prepared to accept as a risk and these risks are defined to be below the *risk appetite* (para19, bullet 1). Risks above the risk appetite require the application of *internal controls* to manage the risks to below the risk appetite (para. 25). The risk appetite and responses shown in the risk heat map are examples only; it is the responsibility of the board to decide on the appropriate response.
- Risks before controls are applied are known as *inherent* and after controls are applied are known as *residual* (para 29 and para. 34, bullet 2).
- The board will define the combinations of impact and likelihood which represent a serious threat to the achievement of the company's objectives and therefore its going concern basis of accounting. It is these risks which are considered as *principal risks* (noted as 'unacceptable' in the risk map) (Main principle C.2, para. 19, bullet 3 and para. 26).
- There are other risks above the risk appetite which are not considered principal risks (further comments later).
- *Material uncertainties* (Code provision C.2.1, para 5, bullet 6 and appendix C) arise where the responses to an inherent principal risk fail to bring the resultant residual risk to below the risk appetite.
- *Severe distress* is caused by a residual principal risk remaining in the area designated as *unacceptable*. This would result in closure of the organisation or would stop it achieving a major part of its objectives for a long period if it materialised. This might require a declaration that the going concern basis of accounting is not appropriate (appendix C).

Risk management terms are defined by *ISO Guide 73:2009 Risk Management - Vocabulary*. The terms I have used are generally consistent with this but the FRC may wish to adopt the ISO vocabulary in the guidance.

I hope to show that the explanation of terms used at the start of the guidance enables later simplification. I don't believe that their inclusion violates the principles noted in paragraphs 10 and 11 which aim to ensure flexibility in implementing the risk management framework.

Mention of objectives?

4. Principle C.2 of the revised code states, *The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems*.

   The draft guidance makes little reference to the link between risks and the threat to the company's strategic objectives. Paragraph 19, bullet 3, hints at it. The first definition of a principal risk, such as it is, is in paragraph 26, which makes no mention of the threat to the strategic objectives, although it does mention 'future performance, solvency and liquidity' which are hopefully included in strategic objectives. The definition at the beginning of appendix B makes no mention of the failure to achieve strategic objectives but refers to 'severe distress' which is expanded in appendix C, which doesn't mention objectives. If a business doesn't know its objectives it cannot determine its risks. I've suggested amendments to emphasise the link between risks and objectives.

Questions posed in the consultation

The FRC would welcome views on whether the additions [to C.1 and C.2] are required and, if so, on the detailed wording; and on whether the existing Provision C.1.3 (on the going concern statement) should be removed.

5. I'm going to answer the last question first, since it raises an important point which runs through the guidance. The main principle to C.2 replaces the word *significant* by the word *principal* to make it consistent with the Companies Act. This is understandable but although *significant* can be taken to refer to all risks above the risk appetite; the generally accepted definition of *principal* is that it only refers to those likely to threaten the going concern basis of accounting. The number of these risks is less than 50 in a typical company's annual report.

6. What about the risks above the risk appetite which are not principal risks? Examples of such risks are: classification of revenue expenditure as capital; payment for goods or services not received; corruption of files by a computer virus. Tesco makes mention of these types of risks in its 2013 annual report (page 38 and underlined in this extract): *The table below sets out the principal risks faced by the Group, and examples of relevant key controls and mitigating factors. The Board considers these to be the most significant risks faced by the Group. <u>They do not comprise all the risks associated with the Group</u> and they are not set out in any order of priority. Additional risks not presently known to management, or currently deemed to be less material, may also have an adverse effect on the business.* The number of these risks will be in the thousands. I am assuming that the guidance does not consider these risks to be included as subsidiary risks within the principal risks, since this is not stated.

7. Does the guidance now only apply to principal risks and not those in the gap between principal risks and the risk appetite? Since section 4 of the guidance is titled *Identifying and*

Assessing Principal Risks and paragraphs 31, 37 and 38 refer specifically to principal risks, this is presumably true.

8. I believe this is a retrograde step. In practice, directors, usually through the audit committee, need assurance that all risks are being controlled to below their risk appetite and be informed where this is not the case. The FRC *Guidance on Audit Committees* section on *internal controls and risk management systems* makes no mention of principal risks. Some of the risks below principal present threats which could result in stopping the organisation achieving its some of its objectives for a limited period and therefore suffering material losses or incorrect accounting. I would also argue that until the company has determined the risks above the risk appetite, it cannot be reasonably sure it has identified all the principal risks. The code and guide need to assign responsibility for the control of all risks, while emphasising the importance of principal risks.

9. The main principle needs to be reworded to take account of this responsibility. The word *principal* should be omitted from the main principle, which would make the board responsible for all risks it is willing to take in achieving its strategic objectives - that is those risks above the risk appetite. In practice, this is no different from the current situation, since these risks are assumed to be *significant*. Thus main principle C.2 should read *The board is responsible for determining the nature and extent of the risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management systems.*

10. Code provision C.2.1 should still refer to principal risks, but I would prefer it to read:

    The board should carry out a robust assessment of the risks that would threaten the company's ability to continue to adopt the going concern basis of accounting ('principal risks'), including those that would threaten its solvency or liquidity. In the annual report the directors should confirm they have carried out such an assessment and explain how the principal risks are being managed. They should indicate which, if any, are material uncertainties in relation to the company's ability to continue to adopt the going concern basis of accounting.

    The new C.2.1. still requires the board to report on those risks which threaten its ability to adopt the going concern basis of accounting but includes a definition of *principal risks*. I've omitted the word *mitigate*, since this is included in *managed*.

11. If the main principle refers only to principal risks, does C.2.2. refer only to those risk management systems covering principal risks? In other words, the board only need to monitor the systems managing the principal risks and not those above their risk appetite? The phrase *risk management and internal control systems* is used throughout the guidance but it is not clear whether these systems now only relate to principal risks or all risks. I think this point needs clarification and suggest the wording; *The board should monitor the systems which manage all the risks which they consider a threat to the achievement of company objectives. At least annually they should carry out a review of the effectiveness of these systems and report to shareholders that they have done so.* I have omitted the last sentence since it is covered by the phrase *all the risks...*and the phrase *material controls* needs defining if it is to be used. My amended C.2.2 is still consistent with Provision C.3.2.

12. The Financial Reporting Review Panel in its 2012 annual report noted the confusion in some company reports over the definition of principal risks. The existence of risks which are of concern to directors (those above their risk appetite) but are not principal risks may add further confusion. The code and guidance need to ensure this confusion does not continue and my comments on the draft guidance (below) try to clarify the difference.

13. In conclusion, I think that the additions are required and C.1.3 should be removed. However, the main principle should apply to all risks and my comments on the draft guidance reflect this view.

The FRC would welcome views on whether the draft revised guidance achieves these objectives [on page 3], and on the structure of, and level of detail in, the draft revised guidance.

14. I think that the draft revised guidance does partially achieve the objectives listed under section 2 (Guidance on risk management and internal control) but it could do better if there were greater clarity and consistency in the terminology used. I've provided more details above and below. Under this question I am providing comments on section 1 of the guidance.

Comments on Section 1

15. ***Para. 2.*** The term *principal risks* is used without any definition. I would include the phrase; *principal risks are those risks which, if they occurred, would threaten the company's ability to continue to adopt the going concern basis of accounting, including those that would threaten its solvency or liquidity.* Thus principal risks are those risks with a high impact and likelihood on the risk heat map.

16. ***Para. 2.*** This paragraph refers to *...board and management respond promptly to risks* but then *shareholders and stakeholders are well informed about the principal risks*. Thus the paragraph seems to recognise the difference between principal risks, which are communicated to shareholders, and other risks which also require a response.

17. ***Para 4*** includes the phrase *risk management and internal control*, which is tautology. I won't mention it again.

18. ***Para 5 bullet 4*** contains the phrase, *managed and mitigated*. As noted in my comment 3, *managed* usually refers to the four methods of reducing risk, which includes mitigation. The *Orange Book: Management of risk - Principles and Concepts* from HM Treasury lists the four methods as below (para. 1.4 of the book) and uses the term *response* instead of *management*.

    Response, which is initiated within the organisation, to risk is called "internal control" and may involve one or more of the following:

    - *tolerating the risk;*
    - *treating the risk in an appropriate way to constrain the risk to an acceptable level or actively taking advantage, regarding the uncertainty as an opportunity to gain a benefit;*
    - *transferring the risk;*
    - *terminating the activity giving rise to the risk.*

    You could do worse than use than use this terminology, so I will.

19. ***Paras. 8 and 9*** confuse me. Para 8 states*, This guidance uses the term "going concern" specifically to refer to the basis of preparation of the financial statements as defined in accounting standards, which is different from the ordinary English usage of the term "going concern".* Para 9 states, *The FRC has developed the guidance on the basis that boards should make clear in their reporting of principal risks which of them are a potential threat to solvency or liquidity (which we consider to be a more common interpretation of the term*

"going concern" risks). So you've developed the guidance using one basis but the guidance published uses another basis?

20. ***Para 9.*** Why single out solvency and liquidity risks? Principal risks are by definition those which threaten the going concern basis of a company. The rapid disappearance of the *News of the World*, although not an independent company, showed that a solvent, liquid business could disappear overnight if it didn't manage its risks.

Do you agree or are more substantive changes to these [2 to 6] sections required?

Comments on Section 2

21. I think changes are required to aid clarification and consistency. In particular paragraph 19 sets the scene for the rest of the guidance but is incomplete and not specific. For example:

    - The need to have clear strategic objectives is not stressed.
    - Risk appetite is mentioned but this implies a system of assessing risks, for example using impact and likelihood measures. However there is no responsibility defined to set up a measurement system.
    - There is no requirement to record risks in a register. Risks need to be recorded in order that they can be ranked by threat and updated.
    - There is no recognition that the principal risks to be identified must be those before taking into account any controls mitigating them.

22. ***Para 19.*** The first, additional, bullet point should be, *Ensure the company's strategic objectives are clear and communicated to all staff*.

23. ***Para 19.*** The second, additional, bullet point should be, *Establish the parameters by which risk is to be assessed (usually impact and likelihood) and how these parameters are to be measured (for example on a scale of 1 to 5) such that risks can be ordered in terms of their threat.*

24. ***Para 19, first bullet.*** To be amended: *determining the extent to which the company is willing to take on risk<u>, expressed in terms of the parameters noted above, such that risks can be assessed as being above or below the company's risk appetite.</u>*

25. ***Para 19, third bullet.*** Add *inherent* to before *principal risks*. Delete from *to the company's*... Principal risks by definition threaten the business model etc.

26. ***Para 19, fourth bullet.*** Amend to, *agreeing how these risks should be <u>tolerated, treated, transferred or terminated</u>.*

27. ***Para 19.*** Additional bullet: *ensuring there is a means of recording risks, such that their level of threat can be determined and changes to risks can be noted immediately and assessed for threat.* Tesco in its 2013 annual report (page 38) makes specific mention of risk registers and it is difficult to see how a proper risk management system could function without such registers.

28. ***Para. 20.*** Why single out solvency and liquidity risks? Public opinion is now a very important factor when considering a company's going concern basis. Loss of public confidence, as a result of phone hacking, loss of customers' financial data, horsemeat contamination or an ecological disaster for example, could bring a solvent and liquid company down overnight. Any principal risk, not properly controlled, threatens a company's going concern basis.

29. ***Para. 21.*** The board cannot be expected to identify all risks above the risk appetite and record them. So add the responsibilities *identify, record* before *implement and take...*

Comments on Section 3

None

Comments on Section 4

30. ***Para. 25.*** As noted in comment 6, the guidance does not recognise that there are many risks above the risk appetite which are not principal risks. Directors must have assurance from management that these risks are being controlled to below their risk appetite and be informed where this is not the case. Without a determination of all inherent risks above the risk appetite, which must involve management, some principal risks in specialist areas (such as IT) might be missed.

    I suggest that the title to section 4 omits the word *principal*. Paragraph 25 could read, *The board and management should identify the ~~principal~~ risks facing...*

31. ***Para. 26.*** This paragraph singles out solvency and liquidity risks. I would suggest it is amended to, *The board needs to be aware of those inherent risks or combination of risks that will have a catastrophic or major impact sufficient to close the company, or a significant part of it, or to prevent the organisation achieving a major part of its objectives for a long period, and which are likely to occur without controls in place. The board should treat such risks as principal risks and establish clearly the extent to which they are to be tolerated, treated, transferred or terminated.*

32. ***Para. 28.*** This paragraph uses the phrase *potentially significant risk* but the word *significant* has been replaced by *principal* in the code, so what does this phrase now mean? Would the sentence be better phrased as, *...other conditions in which inherent principal risks may arise*.

33. ***Para. 29.*** contains the phrase, *extent to which there are residual risks even where these are operating effectively*. There are *always* residual risks; it's just that they are below the risk appetite where the response is effective. I would reword the paragraph as, *Since principal risks threaten the going concern basis of the company and therefore the strategic objectives, the directors should ensure that responses are in place to reduce the threat to below their risk appetite*.

34. ***Para. 30.*** I don't understand the need for this paragraph. As I have said above, I don't believe that the principal risks threatening solvency and liquidity need special mention. Further, the paragraph introduces the concept of *severe distress* which requires over a page of explanation in appendix C. If the risk heat map is used, *severe distress* is simply where the residual risk is in the area designated for *principal risks*.

Comments on Section 5

35. ***Para. 31, first bullet.*** This point fails to acknowledge that there are risks, other than principal risks, above the risk appetite (see comment 6). It also refers to significant control failures, with no attempt to define the phrase. The bullet point would be better phrased as, *facilitate the efficient and effective achievement of its objectives by managing all residual risks to below the risk appetite, react to any risks above the risk appetite, identify emerging risks and safeguard its assets.*

36. ***Para 33***. The phrase *significant control failings* would be better expressed as, *residual risks above the risk appetite.*

37. ***Para. 34.*** This paragraph should refer to the heat map to clarify the points made.

Comments on Draft Guidance to Directors applying the UK Corporate Governance Code

38. ***Para 34, first bullet***. After the phrase, *...the higher the risks accepted*, it would be useful to include *(that is the lower the risk appetite)*, in order to stress the link with a phrase already used.

    Para 34, first bullet. The terms *inherent* and *residual* should be added to this bullet. Thus: *The exposure to risks before responses have been applied (inherent risks) and after (residual risks).*

39. ***Para 34, third bullet.*** The word *consequence* should be replaced by *impact* to maintain consistency.

40. ***Para 34, fourth bullet.*** Replace *incidence* with *likelihood* to maintain consistency.

Comments on Section 6

41. ***Para 37.*** Delete the word *principal* before risks. The directors must be informed about the management of **all** risks above the risk appetite. If the word *principal* is to remain, the guidance to audit committees should be amended, otherwise they will still be required to receive reports on all risks. The report does not have to be in detail but should discuss any residual risks (not *significant control failings*) above the risk appetite.

42. ***Para 38.*** Again delete the word *principal*. I would also like to see the word *recorded* after *identified* in order to emphasise the need for a risk register.

43. ***Para 40, third bullet.*** Include *project management* after business planning processes because this is one activity that can easily fail to deliver what it promises, with expensive results.

44. ***Para 40, fifth bullet.*** I'd prefer this to read, *the scope and quality of management's ongoing identification, recording, monitoring....* This emphasises that management have a responsibility to identify risks, particularly those below principal risks.

45. ***Para 40, seventh bullet.*** It's that *significant control failings* phrase again! I know the phrase *residual risks above the risk appetite* is clumsy but at least it's objective.

Comments on Section 7

46. ***Para 41.third bullet.*** Reference is made to *risk management and internal control system*. Does this system cover all risks or only principal risks? If it covers all risks then surely this guidance should cover all risks? However ***paragraph 51*** refers to an ongoing process for principal risks.

47. ***Para. 57*** **states** *that the board should ... acknowledge that it is responsible for that [risk management and internal control] system...and disclose that there is an on-going process for ... managing the principal risks...*Does this mean that the risk management system only applies to principal risks, or that it applies to all risks and within that system there is a process specific to principal risks?

The FRC would welcome views on this [explain actions para. 58] proposed change to the guidance.

48. ***Para. 58*** refers to *significant failings or weaknesses* with no guidance as to what these might be. I suggest that the second sentence read: *Where the review identified principal risks which were not properly managed and therefore threatened the going concern basis of accounting, the board should explain what actions have been or are being taken to reduce the threat to a level it considers acceptable.* The third sentence will start: *The board should include the process...*

The FRC would welcome views on whether these appendices [D and E] are of use to directors and, if so, how they might be improved.

49. If directors don't find them useful, I'm sure risk managers and internal auditors will.

50. I'd include the following questions under *Risk Assessment*

- Has a means of ranking risks been established so that their threat, before and after controls, can be assessed in relation to the board's risk appetite?
- Are risks recorded in a register, which is regularly maintained to ensure changes to risks are noted?

51. I'm not sure that appendix E is worthwhile. The directors who need to read it probably won't, as one warning sign is that directors aren't aware of the warning signs. I'd incorporate this appendix into appendix D, rewording as necessary.

Do you believe that the approach taken in Appendix B of the draft revised guidance is appropriate? If not, how should it be amended and why?

52. The definition of solvency and liquidity risks contains the phrase *severe distress* which requires an explanation lasting a page in appendix C and starts with *What constitutes severe distress is a matter of judgement*. That's not a good definition.

53. The section on stress testing is too detailed for the guidance. It is inconsistent with the level of detail used elsewhere, particularly the absence of an introduction to explain the basic terminology and concepts of risk management.

54. Since appendix B and C are so closely linked I would combine them.

Do you agree with the guidance in Appendix C of the draft revised guidance? If not, how should it be amended and why?

55. I find appendices B and C difficult to understand. There doesn't seem to be a logical flow; the term *severe distress* is introduced, which is not linked to the concept of impact; and the language used is inconsistent (the paragraphs under *Determining whether there are material uncertainties* use *potential magnitude, possible implications* and *magnitude of their potential impact* to mean *impact*).

56. The only amendment I can suggest to appendices B and C is to rewrite them in the straightforward format and language of the rest of the guidance.

Do you agree with the revised [banking] guidance? If not, what needs to be amended and why?

57. No comment

Do you agree with the draft revised auditing standards? If not, what should be changed and why?

58. No comment, other than amendments I have suggested to the code should be incorporated.

The FRC would welcome views on whether the additions [to C.1 and C.2] are required and, if so, on the detailed wording; and on whether the existing Provision C.1.3 (on the going concern statement) should be removed.

Answered as the first question.

Conclusions

My comments above refer to four main concerns:

59. **The need for an introduction to risk management terminology.** Without an introduction explaining the terminology used and showing the relationship between the terms used in risk management, there is a danger that the guidance is misinterpreted.

60. **The limitation of the guidance to principal risks**. If the guidance now only applies to principal risks, I think this is a retrograde step. If it is still intended to apply to all risks, amendments which stress this are required. I am very confused as to whether the phrase *risk management and internal control systems* refers only to principal risks or all risks.

61. **Consistency of terminology**. I appreciate that the document is intended as guidance for directors and not as a technical accounting standard. Some of my suggested amendments may therefore be considered as nitpicking. However, the guidance will be used to determine the information given to shareholders and other parties dependent on the financial stability of the company and a balance must be struck between readability and technical accuracy. The Financial Reporting Review Panel in its 2012 report indicated some companies are confused over the definition of principal risks and I don't think the guidance will do much to remove it. It does not clearly define many of the terms used, nor uses them consistently. I have tried to remedy this by inserting terms and definitions used for risk management, hence the nitpicking.

62. **Appendices B and C.** These are not written with the same style and clarity of the rest of the guidance. They introduce new, unnecessary terminology, go into unnecessary detail and do not use terms consistently. They deal with important topics and need rewriting.

Yours sincerely

David M Griffiths Ph D, FCA

www.internalaudit.biz

www.managing-information.org.uk