Institute of Risk Management

Financial Reporting Council

Proposed Revisions to the UK Corporate Governance Code

Consultation Paper dated December 2017

Response from the Institute of Risk Management (IRM)

Institute of Risk Management
2nd Floor, Sackville House,
143 - 149 Fenchurch Street
London EC3M 6BN

19 February 2018

Nicola Crawford
Chair
Institute of Risk Management
2nd Floor, Sackville House
143-149 Fenchurch Street
London EC3M 6BN

chairman@theirm.org

Ian Livsey
Chief Executive
Institute of Risk Management
2nd Floor, Sackville House
143-149 Fenchurch Street
London EC3M 6BN

Ian.livsey@theirm.org

Institute of Risk Management (IRM)

The IRM is the leading professional body for risk management. We drive excellence in managing risk to ensure organisations are ready for the opportunities and threats of the future. We do this by providing internationally recognised qualifications and training, publishing research and guidance, and setting professional risk management standards.

We are a not-for-profit body, with members working in all industries, in all risk management disciplines and in all business, private and public sectors around the world. The IRM has a membership in excess of 6,000 risk management professionals and represents a larger risk community in excess of 20,000 on LinkedIn and other social media groups.

Process for developing this response

The process for developing this response was based on discussions with a number of senior UK based IRM members with oversight from the IRM Board.

IRM and corporate governance

IRM believes that Enterprise Risk Management (ERM) is a fundamentally important component of good corporate governance. Exposure to risk is inevitable for all types of organisations, but the level of risk exposure must be within the risk capacity of the company and should be aligned with the risk appetite of the company.

IRM believes that reporting on risk management should reflect how the company embeds risk management within the development and implementation of strategy. Reports should provide an accurate and insightful account of the quality of the risk discussion at board level. IRM also believes that an important part of the purpose of effective corporate governance is to ensure that excessive and/or inappropriate risk taking is avoided.

Accordingly, IRM is pleased to have the opportunity to respond to this Financial Reporting Council consultation paper (dated December 2017) on proposed revisions to the UK Corporate Governance Code. IRM wishes to offer general comments in relation to Section 1 and Section 4 of Appendix A – Revised UK Corporate Governance Code, Paragraph 71 of Appendix B – Revised Guidance on Board Effectiveness and offer specific comments in relation to Questions 3, 7/8, 12 and 13.

UK Corporate Governance Code (Appendix A)

Section 1: Leadership and purpose

IRM general comments

Revision of the UK Corporate Governance Code is an opportunity for the Financial Reporting Council to develop requirements that will ensure that consideration of risk and risk management becomes embedded within the board conversation.

The IRM believes that Section 1 does not pay sufficient attention to risk and risk management. Management of risk is fundamentally important to the success of a company. Risk management should be highlighted in Section 1, rather than being linked to audit and internal control in Section 4. Given the increasing importance of risk management, the risk management requirements of the code should be moved from Section 4 and incorporated within Section 1.

In more general terms, Section 1 needs to be linked more closely to Section 4. There should be a requirement to report on the processes by which strategy is developed and details of how risk assessment supports the development and implementation of strategy. An indication of the time being spent by the board on reviewing the risk related information would be very helpful in understanding the quality of the board discussion on risk management. The scope of this discussion should also be indicated, including information about the identification and analysis of emerging risks.

IRM believes that the risk management requirements currently included in Section 4 should be transferred to Section 1 of the code. IRM suggests that it is impossible for a board to fulfil leadership and purpose requirements without due regard to the anticipated risks. Principle A in Section 1 discusses the long-term sustainable success of the company and this can only be achieved if robust assessment of risks is undertaken. Principle B requires the establishment of a framework of prudent and effective controls which enable risk to be assessed and managed, but this requirement can only be fulfilled if robust assessment of risks has been undertaken.

The inclusion of risk management activities as part of Section 4 misunderstands and understates the importance of proactive risk management. Whereas the inclusion of risk management activities in Section 1 – Leadership and purpose would indicate that risk management is a proactive requirement and that will enhance the short-term success and longer-term viability of the company.

Given the recent demise of Carillion plc, it is worth looking at its Annual Report and Accounts 2016. There is a list of the principal risks that have been identified (pages 32 to 37), but there is a disconnect between the risk matrix included and the narrative presented in the ‘Viability Statement’ (page 31). The risk management information provided is insufficient to indicate the true health of the company. Pages 30 and 31 give detailed information on the risk management processes in place, but these appear to be based on separate management information that is not used to support board decision-making.

The debt / liabilities risk is not listed as a principal risk by Carillion. Refusal of the banks to continue providing finance was reported as being the reason for the failure of the company. However, the breaching of banking covenants and/or the withdrawal of financial support from financiers was not reported as a principal risk. This observation is not offered as a criticism of Carillion, so much as an indication that for many companies, risk management is treated as a separate activity, not related to the success and viability of the company.

The Carillion risk management reporting is typical of companies that treat 'risk management' as 'list management', where the focus is on the management of the list of risks, rather than utilising risk information to enhance strategy, tactics, operations and compliance activities. No context is provided for the principal risks and no details of the possible impact(s) of risks is provided. Typically, risk / risk management reports in many annual reports take a 'boilerplate' approach to risk reporting.

In the Carillion report, the use of a risk matrix to illustrate how the list of risks can be represented on a simple 2x2 risk matrix is simplistic and unhelpful. If the information on principal risks is presented to the board in this format, the importance of the risk information and its possible impact(s) on the success and viability of the company is unclear. The code requirements should ensure that companies cannot claim compliance based on management of the list of principal risks.

Question 3: Do you agree that the proposed methods in Provision 3 are sufficient to achieve meaningful engagement?

IRM response

The engagement of wider stakeholders and the means of raising concerns by way of whistleblowing is something that the IRM supports. Progressive companies would also have a mechanism for consultation with the workforce to gain better insight into actions that would improve operational efficiency and effectiveness. A comprehensive arrangement that receives and evaluates positive comments, as well as criticisms, should be encouraged. This arrangement should enhance the culture of the company in that a culture of co-operation and consultation will be developed that will add to company success.

Question 7: Do you agree that nine years, as applied to non-executive directors and chairs, is an appropriate time period to be considered independent?
Question 8: Do you agree that it is not necessary to provide for a maximum period of tenure?

IRM response

It is important for non-executive directors to serve only a limited term. The IRM does not have a strong view of whether this should be six or nine years, but the need to have a limited tenure is vitally important. This will help ensure that unchallenged risk-taking or tolerance of unacceptable risks will be reduced. The quality of the board discussion on risk and risk management will be enhanced by the recruitment of new non-executive directors on a clearly scheduled basis.

Question 12: Do you agree with retaining the requirements included in the current Code, even though there is some duplication with the Listing Rules, the Disclosure and Transparency Rules or Companies Act?

IRM response

The corporate governance code should include provisions related to risk, audit and internal control to emphasise the importance of risk management throughout the company. The duplication of these obligations in other documents, can only serve to reinforce the importance of risk management. In any case, the UK Corporate Governance Code is used and applied well beyond companies listed on the stock exchange. Therefore, a more complete account of the scope of corporate governance within the code is supported by the IRM.

Section 4: Audit, risk and internal control

IRM general comments

Combining audit, risk and internal control in Section 4 is inappropriate. Risk management is a separate proactive activity that assists with the formulation of strategy and tactics. Risk management also enhances the efficiency and effectiveness of operations and it proactively enhances compliance activities. Audit, on the other hand, is related to activities that retrospectively check compliance.

Management of risk cannot be based entirely on implementation of the controls, because risk management requires risk identification, especially in relation to emerging risks. Procedures for risk analysis and risk evaluation against risk appetite (or risk criteria) need to be established. It is only after risk assessment has been undertaken that controls can be identified. The emphasis on controls in the code presumes that the correct controls have been implemented. Without robust risk assessment, this presumption is almost certainly going to be incorrect.

The IRM suggests that Principle M should be split. The second half of Principle M "*and satisfy itself on the integrity of financial information.*" should be added to Principle L. The first part of Principle M *"The board should present a fair, balanced and understandable assessment of the company's position and prospects."* should be transferred to Section 1 as part of Principle A on long-term sustainable success.

Risk management information should be used to test strategy, identify and implement projects, improve the effectiveness and efficiency of operations, and as a means of enhancing compliance. If risk management information is to be used in this way, information is required on 'close-calls' and 'near misses'. This will require the development of early warning Key Risk Indicators (KRI's), and establishment of risk limits that are measured against risk appetite. Companies should have appropriate risk management metrics to track the well-being and success of the company and these should be referenced in the guidance to Principle N.

As demonstrated by the Carillion example, the existing requirement to produce a longer-term viability statement has resulted in qualitative generic statements that do not identify the risk assumptions that underpin the statement. The resulting statements are vague and bland.

Ensuring the longer-term viability of a company is part of Principle A in Section 1 and the requirement to undertake robust risk assessment activities should be attached to Principe A. Paragraph 31 of the guidance should be re-located accordingly.

Question 13: Do you support the removal to the Guidance of the requirement currently retained in C.3.3 of the current Code? If not, please give reasons.

IRM response

The IRM believes that the requirement to publish the terms of reference for the audit committee should be retained. In many companies, separate audit and risk committees are necessary and, in these circumstances, the terms of reference of both committees should be published. The terms of reference should include details of the qualifications and relevant experience of members of each committee. These committees should have different chairs and separate meetings. This will ensure that risk management becomes a proactive management activity, distinct from the audit activities with their emphasis on audit findings and discussion of issues that have already arisen.

UK Corporate Governance Code (Appendix B)

IRM general comments

Paragraph 39

The revised guidance on board effectiveness Paragraph 39 states that 'the board sets the framework within which a healthy corporate culture can develop, that underpins the way in which the company operates. It then satisfies itself that the culture throughout the organisation is consistent with that framework, leading by example and taking action where it spots misalignment.' This point could be amended to expressly address risk culture.

Paragraph 71

The revised guidance on board effectiveness Paragraph 71 states that "It is the responsibility of the company secretary to ensure that directors, especially non-executive directors, have access to independent professional advice at the company's expense …" The IRM is of the opinion that the Code should be more explicit in extolling the merits of having risks or the actual risk management system itself reviewed independently.

As an example, the Ministry of Justice Guidance on the UK Bribery Act is much more explicit on this, stating: "…. organisations might wish to consider seeking some form of external verification or assurance of the effectiveness of anti-bribery procedures."

Citing the Carillion case, had they engaged an outsider to review their risks it would have been much more difficult for Carillion to gloss over the existential threat they faced in their reporting to shareholders and other stakeholders.

Ian Livsey
Chief Executive
Institute of Risk Management