The FRC's UK Corporate Governance Code Consultation Document of May 2023

Submission from Airmic

13 September 2023

Introduction

As the association in the UK and Ireland that champions the strategic value of risk management and insurance in a changing world, Airmic is keenly following the revision of the UK Corporate Governance Code. Given the interconnected and fast-evolving nature of risks today, Airmic has been collaborating with bodies such as the Chartered Institute of Internal Auditors (CIIA), the ACCA (the Association of Chartered Certified Accountants) and British Standards Institute (BSI) Committee RM/1 on these issues.

This submission by Airmic is based on consultation with members through a closed-door roundtable held jointly with the CIIA on 5 September 2023, and on research conducted with the ACCA and the Professional Risk Managers' International Association (PRMIA) on *Risk culture: building resilience and seizing opportunities*, published in April 2023. Airmic has also been privileged to participate in the Financial Reporting Council's own report on *Creating Positive Risk Culture*, released in December 2021. Nevertheless, the views and positions presented in this submission should not necessarily be taken to represent the views of those other organisations, of which we understand the CIIA and ACCA are making their own submissions to the FRC.

1. Background: Risk, reporting, and permacrisis

We all find ourselves in a permanent state of crisis today. Risk leaders cannot address all risks and risks cannot be addressed in silos – the world is now so connected, complex and dynamic that everyone must be involved. This scenario demands new risk management tools and techniques, with agility the name of the professional game.

Risk registers and internal audit programmes are inadequate if they are set less frequently than the context demands. Both must be dynamic and operate in unison otherwise a time lag can develop between the activities of assessing risk and the assurance of this. For a realistic, business-driven outcome, the reporting process should determine the output, rather than that we concern ourselves with reporting the output.

Before addressing selected questions specifically as laid out by the FRC in the consultation document of May 2023, we would like to make the following key points:

1. We recommend that the Three Lines Model be referenced in guidance documents to the Code, to enable a better understanding of the role of risk management in relation to internal

audit, and the relationship between them and with the governance and leadership of an organisation.

2. The reasons behind most corporate collapses are behaviour and culture. The ACCA, PRMIA and Airmic have called for risk culture to be measured and incentivised, so that everyone in the organisation owns it. This includes the alignment of remuneration with the organisation's purpose and performance.

Finally, we discuss emerging risks in the last section of this submission. We started this submission by describing the context of an increasingly connected, complex, and dynamic world. This context has stimulated a period of instability and insecurity created by a series of catastrophic man-made and natural events – the permacrisis we find ourselves in. There is a link here to the importance of emerging risks, and we reflect on the need for the Corporate Governance Code and associated guidance to address the 'how' in managing emerging risks, as well as the 'what' and the 'why'.

2. Responses to questions in the FRC's UK Corporate Governance Code Consultation Document of May 2023

Q2: Do you think the board should report on the company's climate ambitions and transition planning, in the context of its strategy, as well as the surrounding governance?

Yes – but while the board should report on the company's climate ambitions and transition planning as well as the surrounding governance, closer scrutiny of the company's climate ambitions and transition planning should be delegated to the audit committee. (See also our response to Question 12 below.)

Care must be also exercised such that the work of the risk committee – and indeed other board committees – not overlap with that of the audit committee.

Q3: Do you have any comments on the other changes proposed to Section 1 (on Board Leadership and Company Purpose)?

We agree with how the proposed changes to Section 1 have been calibrated, in that they do not overly complicate the processes and policies as related to the board in the quest to strengthen the organisation's culture – given that it is behavioural rather than compliance considerations that determine the organisation's culture.

Q7: Do you support the changes to Principle I moving away from a list of diversity characteristics to the proposed approach which aims to capture wider characteristics of diversity?

We support the changes to Principle I moving away from a list of diversity characteristics to the proposed approach which aims to capture wider characteristics of diversity.

While we recognise that many industries still have much progress to make on gender and ethnic diversity, it is imperative in view of the world we operate in that boards are also encouraged to consider diversity in terms of sexual orientation, age and disability, among other protected and non-

protected characteristics. The entire composition of boards has been overhauled at times, especially in the course of the pandemic and its aftermath. We consider this to be healthy if it strengthens diversity and inclusion within the organisation, while maintaining the relevant competencies of those who govern.

We believe the proposed changes to Principle I in no way dilutes the continued importance of driving greater gender and ethnic diversity.

Q10: Do you agree that all Code companies should prepare an Audit and Assurance Policy, on a 'comply or explain' basis?

We agree that all Code companies should prepare an Audit and Assurance Policy, on a 'comply or explain' basis.

Q13: Do you agree that the proposed amendments to the Code strike the right balance in terms of strengthening risk management and internal controls systems in a proportionate way?

We agree with the new Principle (Principle N) which goes further by making the board responsible not only for establishing, but also maintaining the effectiveness of, the risk management and internal control framework.

This broadly conforms to the Three Lines Model (formerly the 'Three Lines of Defence Model'), where:

- The governing body (that is, the board), as it accepts accountability to stakeholders for oversight of the organisation, determines the organisation's appetite for risk and exercises oversight of risk management (including internal control), and establishes and oversees an independent, objective, and competent internal audit function;
- The first line leads and directs actions (including managing risk) and application of resources to achieve the objectives of the organisation;
- The second line provides complementary expertise, support, monitoring, and challenge related to the management of risk;
- The third line (that is, internal audit) communicates independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management (including internal control).

In our opinion, the Three Lines Model best captures the desired balance in strengthening risk management and internal controls systems in a proportionate way. We believe the time has come for guidance on the Corporate Governance to make reference to the Three Lines Model. (See also our response to Question 16 below.)

Airmic supports the use of the Global Institute of Internal Auditor's interpretation of the Three Lines Model in its 2020 iteration, but would place greater emphasis on collaboration between the second and third lines, even as their distinct roles are respected. Risk and internal audit professionals need to collaborate and work more closely together in order to navigate their organisations through the permacrisis, where operational challenges often transform into strategic ones.

Q16: To what extent should the guidance set out examples of methodologies or frameworks for the review of the effectiveness of risk management and internal controls systems?

As discussed above in our response to Question 13, we recommend that the Three Lines Model should be upheld in future guidance documents on the Code that FRC seeks to put forward.

However, this is not to insist on the strict interpretation of just one model, especially if it is recognised that other governance models may be more appropriate for some organisations; neither are we calling for the application of the Three Lines Model on a 'comply or explain' basis. Just for instance, the UK Government's *Orange Book for the Management of Risk – Principles and Concepts* carries a version of the Three Lines Model which takes into account the role of organisations such as the National Audit Office, which public bodies fall under the purview of.

Q12: Do you agree that the remit of audit committees should be expanded to include narrative reporting, including sustainability reporting, and where appropriate ESG metrics, where such matters are not reserved for the board?

While we agree in principle that the remit of audit committees should be expanded to include narrative reporting, including sustainability reporting, audit committees are by nature "backward-looking" rather than future-gazing. Therefore, it is crucial that the board as a whole retains strategic oversight on narrative reporting and sustainability reporting, insofar as it relates to the setting of controls and processes which can impact the organisation's strategy – although we are satisfied that there is nothing in the proposed changes to the Code which militates against this.

Even as Environmental, Social, and Governance (ESG) factors have become essential considerations for organisations around the world today, we caution against an adoption of ESG metrics by default. The recent political backlash against ESG issues in the United States – where a number of states have enacted 'anti-ESG' legislation – have led some of our members to report that their organisations are sometimes caught in a 'damned if you do, damned if you don't' situation with regard to ESG issues, especially when they oversee global operations. On 15 May 2023 for instance, the Attorneys General of 23 US states wrote a letter to 28 insurance companies belonging to the Net-Zero Insurance Alliance, warning them that they could potentially be violating anti-trust laws with regard to their ESG initiatives. This led some insurers to withdrawal from the Alliance.[1]

In a non-US case, a multinational mining company, which withdrew its operations from China for ESG reasons, had its credit rating downgraded by a credit rating agency because of its resultant loss in profit. The company was effectively penalised even though it was 'doing the right thing', because of a lack of coordination between these different metrics.

Nevertheless, the focus of sustainability reporting efforts should be on clear objectives such as net zero targets, decarbonisation and transition planning.

More generally, organisations today also tend to fall into the trap of treating ESG issues as a compliance, tick-box exercise rather than focusing on the outcomes that such principles are meant to deliver. As Airmic's 2023 research on risk culture with the ACCA and PRMIA reveals, regulatory

[1] Reuters, 'Insurers flee climate alliance after ESG backlash in the US,' 26 May 2023. https://www.reuters.com/business/allianz-decides-leave-net-zero-insurance-alliance-2023-05-25/

change is the top risk priority for organisations today, and that most organisations still fail to link risk or ESG with value creation.

Q18: Are there any other areas in relation to risk management and internal controls which you would like to see covered in guidance?

For all risks – not just emerging risks – materiality may be a function of how risks interact with each other. Therefore, the FRC should consider the principle or requirement of understanding how risks influence each other as part of any effective control framework.

The information needed to manage some risks is available in good time and control measures may be detailed and effective control is established with compliance. With other risks, such as security and cyber risk management as examples, the information needed to control some of the associated risk impacts emerges in real time with the risk event. In these circumstances, effective control is dependent on a framework of constraints, within which a trained expert makes the decisions. Using the wrong control style with each type of risk leads to poor decisions and bad outcomes. Control effectiveness therefore depends on knowing what type of risk it is and providing the right style of control.

Q26: Are there any areas of the Code which you consider require amendment or additional guidance, in support of the Government's White Paper on artificial intelligence?

AI risks should not be monitored or addressed in isolation, but as part of all other risks faced by an organisation. As such, the Code should not seek to address specific AI risks, which could instead be dealt with other government policy levers.

As the use of AI is increasingly embedded in more and more applications, regulating AI per se would be impractical and self-defeating. It would be akin to saying that the use of all computers must be regulated. Also, as the development of AI continues at a rapid pace, a Code or any piece of legislation that is updated every few years would not be the most appropriate vehicle for addressing its risks.

More generally, we believe there is a pressing need to cut through the present hype around AI to clearly define what AI application is referred to in any legislation or regulation – whether it is machine learning as contrasted with generative AI, for instance.

3. Emerging Risks

Given the permanent state of crisis and the complex and dynamic world we find ourselves in today, it is imperative that the Corporate Governance Code and subsequent guidance documents address emerging risks – if the Code is to remain relevant for organisations.

Therefore, with regard to the FRC's intended update to the *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting* to be developed later in the year, we are strongly supportive of the FRC's proposal that it covers procedures to identify and manage emerging

risks, and that it emphasises the importance of the risk assessment being a continuous and dynamic process rather than a one-off exercise during the year.

We look forward to the opportunity of engaging more closely with the FRC on emerging risks, especially in the course of the update of the *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*. Ahead of that update to the guidance, we wish to provide the following points on emerging risks for consideration.

Q17: Do you have any proposals regarding the definitional issues?

In the standard *Risk management — Guidelines for managing emerging risk to enhance resilience* (ISO TS31050) which is due to be published by the International Organisation for Standardisation (ISO) in the fourth quarter of 2023; emerging risks are not explicitly defined, but are characterised as "risks for which the body of knowledge to manage the risks, is yet to be fully known."

The FRC should set out the characteristics that organisations should use to identify a risk as an emerging risk. Key to this list is the lack of an established body of knowledge, which can be tested as part of an audit.

The ISO TS 31000 standard sets out the use of three time horizons to capture emerging risks that need immediate attention, emerging risks that are in the medium term and emerging risks that may crystallise (or disappear) in the longer term. These three time horizons help ensure resources are used wisely and appropriate controls are established to manage the risks at each stage. These three time horizons can also be defined by an organisation and tested for validity as part of the Audit process in the same way as the Government expects auditors to test the definitions of short and medium term.

Effectiveness for emerging risks would need to be based on the organisations ability (and agility) to source data, as it becomes available, and transform that data into strategic insight in support of timely decision making. These minimum standards may be set out as a methodology, a framework for emerging risk, or as additional principles.