Quoted Companies Alliance

6 Kinghorn Street
London EC1A 7HW

T +44 (0)20 7600 3745
mail@theqca.com

www.theqca.com

Department for Science, Innovation and Technology
100 Parliament Street
London
SW1A 2BQ
United Kingdom

cybergovernance@dsit.gov.uk

Tuesday 19 March 2024

Dear DSIT colleagues,

Cyber Governance Code of Practice: Call for views

We welcome the opportunity to respond to your call for views on the Cyber Governance Code of Practice.

The Quoted Companies Alliance (QCA) has examined the proposals and advised on this response from the viewpoint of small and mid-sized quoted companies.

The QCA, and our members, recognise the importance of companies and their directors addressing key business risks, including those relating to cyber risks. The frequency and sophistication of cyber attacks has increased significantly in recent years, and they can have a substantial impact on the company itself, as well as their employees, customers, and other stakeholders. As a result, many companies now consider cyber security risks to be principal and material risks for their business, and therefore combine cyber risk management within their existing risk management practices.

Moreover, the two dominant corporate governance codes in the UK have both placed greater emphasis on this area following their recent updates. The new UK Corporate Governance Code (published in January 2024) now requires that boards should establish and maintain an effective risk management and internal control framework, which will mean that the board are formally responsible for cyber risk. Similarly, our Code (the new QCA Corporate Governance Code (published November 2023)) requires the board to ensure that all potential risks are considered on a proportionate and material basis and that the board has the necessary skills and experience to fulfil its governance responsibilities, including with respect to cyber security.

However, practice on cyber governance is often mixed, and it is not always the board who assumes responsibility for the ultimate oversight and management of cyber risk. In this light, we welcome that the Government is aiming to support directors to drive greater cyber resilience.

We broadly welcome the development of the Cyber Governance Code of Practice insofar that it will support directors in improving their governance of cyber risks. In addition, the actions attributed to the five

overarching principles are not unduly prescriptive and have broad applicability, meaning there is flexibility and scope for variation in how companies and their directors choose to apply the principles.

We also welcome that the Code of Practice will be launched as a voluntary tool without its own statutory footing. This will allow companies and board members to adopt and use the Code of Practice in a manner that they see appropriate to the circumstances of their business in order to support and guide their practices and disclosures on issues relating to cyber security. Cyber governance is also an increasing expectation of investors who want to see clear disclosure on the role of the board in this area. This will naturally drive boards to follow, or at a minimum consider, the Code of Practice in their approach to improving their cyber resilience. As such, we consider that the Code of Practice should remain a voluntary tool and that if any change to its status is considered at a later date that this is consulted on with market participants.

It should be noted, however, that some members of the QCA do not consider that another Code of Practice is necessary to encourage people to focus on key business risks. It is the view of these members that this could result in the board spending more time focussing on reputational risk management in order to claim something has been done, taking focus away from addressing other relevant issues.

Moreover, the Government should ensure that there are sufficient levels of professional standards and training courses in place to ensure directors can develop the necessary skills and capabilities to be able to ensure they are effective in their role when it comes to cyber security. Issuing the Code of Practice without a sufficient supply of standards and professional training courses will not result in the outcomes that the Code aims to achieve.

If you would like to discuss our response in more detail, please do not hesitate to contact us.

Yours sincerely,

James Ashton
Chief Executive