Foreword: Viscount Camrose

The UK has a world leading reputation in cutting edge technologies which is underpinned by a pro-innovation approach to tech regulation. As the digital economy continues to grow at an exponential rate, so does society's dependence and global interconnectivity. This presents benefits but also challenges. We know that malicious actors pose a significant threat, seeking to capitalise on opportunities that exploit cyber security vulnerabilities in digital systems, disrupting business continuity and causing economic harm.

The growing use of emerging technologies, such as artificial intelligence, across organisations has elevated the importance and necessity of directors' taking action on how to govern their implementation, harnessing their power to capitalise on the advantages they provide, while appropriately managing and mitigating their risks. Governing digital and cyber security risk effectively is not only fundamental to building a secure and digital economy, it is integral to organisations' business continuity and competitiveness. Boards and directors should therefore place the same importance on governing cyber risk as they do with other principal risks.

The UK is taking the lead in the technologies vital to being a cyber power, while strengthening resilience at a national and organisational level to prepare for, respond to and recover from cyber attacks. Which is why, backed by £2.6 billion pounds of investment, the government's National Cyber Strategy sets out how we are building a prosperous and resilient digital UK which will contribute to driving up cyber resilience standards.

Organisations have a responsibility to take action to manage their own cyber risk but stronger frameworks of accountability and good governance are needed at board level to make this a priority. This requires boards and directors, of organisations of all sizes, to embrace, engage with and understand cyber security within their own organisations. It is in this context that the government sees business resilience and cyber security as intrinsically linked. By neglecting basic cyber security principles and not understanding cyber in the broader context of business resilience, many senior leaders are failing to take responsible action to mitigate threats to business operations.

I am therefore pleased to introduce this call for views on a Cyber Governance Code of Practice, which will support directors to drive greater cyber resilience. This code is the product of extensive engagement with organisations that manage and advise on business risk on a daily basis, and has been co-designed with industry leaders and technical experts at the National Cyber Security Centre. I would like to put on record my thanks and gratitude to those who have so generously given up their time over recent months to help develop the draft code which you now see before you.

The code focuses on the most critical areas that leaders must engage with, forming simple, actions-focused guidance, making it easier for directors to understand what actions to take. This is an integral step in supporting boards and senior leaders to take better accountability for their cyber risk.

Your engagement with the questions in this call for views will help the Government develop plans to build a safer and more prosperous UK. I encourage all organisations with an interest in corporate governance, cyber risk management, board engagement and cyber resilience to take part. We welcome views from all sectors and business sizes. From academics, organisations without formalised boards, to organisations who procure or outsource cyber security, and other interested parties.

I look forward to continuing discussions on how the government and industry should prioritise efforts to bolster the UK economy's cyber resilience. I thank you in advance for your contribution to this vital aspect of our national security.

Viscount Camrose

Parliamentary Under Secretary of State, Department for Science, Innovation and Technology

Cyber Governance Code of Practice call for views

Introduction

The vast majority of organisations in the UK rely on digital technologies to create and conduct business operations. As the digital economy grows, so too do cyber security risks, which are a principal risk to many companies. Greater digital operations provide opportunities for malicious actors to exploit vulnerabilities in IT systems and disrupt business continuity. Organisations are now more than ever before at risk of being disrupted and suffering both malicious and accidental material incidents.

This relatively new risk environment is dynamic and more fast-moving than traditional business risks. Cyber security risk faces a multiplier effect of (i) the pace at which businesses are digitising and transforming operations, (ii) the increasing interconnectedness of digital supply chains, (iii) an evolving threat landscape where state and non-state actors seek to exploit new vulnerabilities created by increased digitisation and connectedness. This is further complicated by a rapidly evolving set of regulatory frameworks domestically and internationally.

Cyber incidents can have severe impacts on organisations of all sizes, both in the short and longer term, from causing business interruption and reputational damage, to being paralysed by ransomware and unable to recover financially. Forbes 2023 explains that 'cyber risk is no longer just an IT problem, it is a critical vulnerability that directly influences the health of the collective enterprise.'

Given its impact, and materiality to business continuity and competitiveness, cyber risk should have the same prominence as financial or legal risks. In today's increasingly digitally dependent economy and society, directors should entwine cyber risk management with existing business resilience and risk management practices. This requires boards and directors, of organisations of all sizes, to embrace and engage with cyber security and understand the risk that cyber incidents present to delivery of the business strategy. It is in this context that the government sees business resilience and cyber security as intrinsically linked.

Governance in a technology age

Digital technologies now underpin business resilience and cut across so many organisational and strategic areas of the business, from strategy definition and capability building to partner selection or business integration. Executive and Non-Executive Directors therefore need to take greater action to provide stronger governance on technology strategies. Clear leadership, and becoming skilled at governing technology, both capitalising on its opportunity as well as managing risks associated with its adoption and use, is fundamental to doing business today. Management and leaders therefore need to ensure that there is a coherent and practicable strategy which weighs up various interdependencies between competition and risks of security, safety, ethics and reputation.

Whether governing of technology issues is done via regular engagement as a recurring agenda item or informal engagement on selected topics, it is critical that executive and non-executive directors develop their understanding and prioritise technology decisions whilst appropriately considering the risks to their business strategy.

Cyber governance and ensuring the organisation's resilience to cyber security risk is one part of this broader environment of technology governance. Cyber governance focuses on a top-down approach to managing and mitigating risks associated with security concerns of the organisation's use of digital technologies.

What is cyber governance and why is it important?

Better governance of cyber security risk is critical to improving the cyber resilience of organisations and better protecting the UK economy and society. Our evidence suggests that a focus on improving the governance of cyber security within an organisation often leads to the fastest improvements in overall cyber resilience (Cyber Security Breaches Survey 2023). Improving cyber resilience forms part of one of the objectives of the National Cyber Strategy, which sets out the government's commitment to strengthening resilience at national and organisational level to prepare for, respond to and recover from cyber attacks. This approach to cyber resilience is absolutely critical in order to ensure:

I. Cyber resilience is embedded within company strategy and integrated across all relevant business processes, not just the IT or technology domains; and
II. Responsibilities for the management of cyber resilience are clear and are embedded across all relevant domains to ensure they are not siloed.

To govern cyber risk effectively, organisations need to implement a top-down approach. This requires the most senior leaders of an organisation, whether that is the directors, board or equivalent, to take ownership of cyber risk, understand the threats that the organisation faces and assess what action is being taken to manage them.

International approaches to cyber governance

Globally, a number of other countries are prioritising cyber governance and are driving greater engagement and action from directors, including the US through its SEC rules, which require boards to have oversight of risks from cyber security threats. Recently, industry associations, including the US' National Association of Corporate Directors and the Australian Institute of Company Directors, have published key principles to support directors in meeting the requirements of their national regulatory frameworks. This demonstrates the growing expectations of directors in grappling with this new form of risk governance. The US National Institute of Standards and Technology has recently launched the first draft of its

Cybersecurity Framework 2.0 with the most notable addition being a sixth pillar focusing exclusively on governance. The recent activity around cyber governance demonstrates a collective refocusing on this process, particularly around individuals' roles and responsibilities in an organisation's cyber risk management posture.

Standards and guidance landscape

There are a number of government and industry-led resources that already exist to help support business leaders. In 2019, the National Cyber Security Centre published the Cyber Security Toolkit for Boards and earlier this year issued a revised version ensuring it remains relevant to the current cyber security landscape. The Toolkit is designed to improve board members' and senior leaders' confidence in discussing cyber security with their key stakeholders across the business and help them make informed decisions about cyber risks and cyber security within their organisation. Despite this, the Cyber Security Breaches Survey 2023 found that board engagement has continued to decline among businesses since 2021. Findings from the Cyber Security Incentives and Regulation Review Call for Evidence 2020 demonstrate that there remains demand for further support from the Government to clearly set out what good looks like for governing cyber risk.

The National Cyber Security Centre's Cyber Assessment Framework furthermore articulates outcomes expected of regulated companies and including areas of governance such as board direction and assurance.

Across industry, there are a number of best practice standards, particularly in IT operations, security operations and enterprise risk management, but less so when it comes to governance and providing directors or boards with direction. When looking across the breadth of standards and guidance, it is clear that the majority do not specifically target directors and therefore do not use language that they are familiar with. In addition, the majority are also predominantly outcomes focused which can be difficult to interpret and implement without a reasonable understanding of cyber security.

As demonstrated above, collectively, the current standards and guidance landscape has not led to sufficient action being taken by directors on foundational cyber governance issues to keep pace with this changing risk environment.

Regulatory environment

Cyber security regulation

The government has sought to put in place a regulatory framework for cyber security, including data security, that is balanced and sufficiently flexible, so that organisations ensure they protect themselves, their suppliers and partners, and their customers from the harms associated with cyber security risks. The regulations that the government has introduced, such as the Network and Information Systems

Regulations, and the UK General Data Protection Regulation (GDPR), complemented by sector specific regulations, set out the requirements and supporting guidance to explain the measures that organisations are expected to implement.

The Cyber Assessment Framework was developed as a tool to support effective cyber regulation. As mentioned above, this defines wide ranging outcomes to achieve effective cyber governance, relevant to regulatory requirements under the Network and Information Systems Regulations.

Beyond cyber regulation, the UK GDPR is a whole-of-economy driver of effective data security. Article 5(1)(f) and Article 32 set out that personal data shall be processed in a manner which ensures appropriate security using appropriate technical and organisational measures. The Information Commissioner's Office (ICO) has explained in guidance that organisational measures equate to key governance actions including, but not limited to, conducting risk assessments, clear and coordinated accountabilities and responsibilities, and developing a culture of security awareness. Despite this, some directors are not taking responsibility for ensuring that these actions are done. In October 2022, the ICO issued a fine of £4.4 million against Interserve, a Berkshire based construction company, for failing to keep personal information of its staff secure by not putting in place appropriate technical and organisational measures as required by Article 5(1)(f) and Article 32.

UK company law and Corporate Governance Framework

UK businesses are also subject to broader statutory and other regulatory requirements covering risk management, such as contained in the Companies Act 2006, and for premium listed companies, the UK Corporate Governance Code, which should influence the way organisations manage their cyber risk. The Companies Act 2006 currently requires all large companies to provide an annual "description of the principal risks and uncertainties facing the company." While useful, this existing requirement does not require information on how such risks and uncertainties are being addressed and mitigated, their likelihood and potential impact, the time period over which they are expected to last, and companies' underpinning governance processes for risk management and developing business resilience.

The Corporate Governance Code sets best practice in relation to governance and is supported by guidance including Risk Management, Internal Control and Related Financial and Business Reporting. This guidance articulates the duty of the board in risk management. Directors must both design and implement appropriate risk management and internal controls systems that identify the risks facing the company and enable the board to make a robust assessment of the principal risks. We now live in a digital world where for most organisations cyber security is either a principal risk, or is relevant to an organisation's management of principal risks, given that having access to digital systems is crucial to creating value and maintaining

business continuity. To enhance the Corporate Governance Code's effectiveness promoting good corporate governance in the context of business today, the Financial Reporting Council (FRC) has recently run a consultation which proposes that the board make a declaration that the company's risk management and internal controls systems have been effective throughout the reporting period. This consultation ended in September 2023 and it is expected that both the Corporate Governance Code and associated Guidance will be updated following feedback received, and we will work to ensure consistency with our Code of Practice.

Current UK cyber governance

The Cyber Security Breaches Survey 2023 found that while cyber security is seen as a high priority by senior management at 71% of businesses and 62% of charities, this has not translated into action or greater ownership of cyber risk at the most senior level. In addition, only three in ten businesses (30%) and charities (31%) have board members or trustees explicitly responsible for cyber security as part of their job role. Qualitative insights from the same survey show a similar set of issues to previous years that prevent boards from engaging more in cyber security, including a lack of knowledge, training and time.

One example of insufficient director involvement is demonstrated in less than half (47%) of medium organisations and only 64% of large organisations having a formal incident response plan in place (Cyber Security Breaches Survey 2023). Given the criticality in responding to incidents quickly, directors should be ensuring that their organisation has an incident response plan that is tested at least annually, so that when it is needed it can be put into action at pace.

A second critical aspect of cyber governance lies with who is involved across the organisation. A Marsh global survey of more than 1,300 executives examined cyber risk and management strategies and found that 70% of respondents named the IT department as a primary owner and decision-maker for cyber risk management, compared to 37% who cited the C-suite and 32% their risk management team. A bottom-up approach where the CISO or equivalent is left responsible for governing cyber risk as an enterprise wide risk is not conducive to developing business resilience. It is the responsibility of directors to ensure that the company's technology stack and associated risks are interwoven with the organisation's mission, strategy and objectives. This requires directors to have regular two way dialogue with the CISO or key risk owner(s), as well as convening and engaging with others across the organisation who are also responsible for managing and considering cyber risks, for example, the HR or Strategy director. Governing cyber risk in this way allows organisations to take full advantage of digital technologies which fuels innovation and drives their competitiveness.

Proposed approach: Cyber Governance Code of Practice

Despite the existing regulatory requirements and supporting guidance and tools, organisations that responded to the Cyber Security Incentives and Regulation Review Call for Evidence 2020 said that they find the cyber landscape complex and challenging to navigate, with 83% of those surveyed stating that there is a need for additional solutions to illustrate 'what good looks like' for governing cyber risk. This view has been strongly supported in the engagement the government has had on governing cyber risk over the past twelve months with a range of organisations, including auditors and industry bodies.

This helps demonstrate that whilst resources on how to govern cyber risk more effectively do exist, they can be hard to find and engage with. In addition, the majority of existing resources are predominantly outcomes focused which can be difficult for directors to engage with when having limited time and limited understanding of cyber risk.

While there is no one size fits all approach to governing business risks such as cyber risk, there are some common fundamental actions that all directors and their organisations should take. **A Cyber Governance Code of Practice, as proposed here, would bring together the critical governance areas that directors need to take ownership of in one place, in a form that is simple to engage with, for organisations of all sizes.**

A Cyber Governance Code of Practice would formalise government's expectations of directors for governing cyber risk as they would with any other material or principal business risk.

Purpose and scope of the call for views

The scope of the call for views is focused around three particular issues:

- the design of the Cyber Governance Code of Practice;
- how the government can drive uptake of its use and compliance with the code; and
- the merits and demand for an assurance process against the Code.

Design

A draft Code of Practice has been co-designed with a range of governance experts including but not limited to, Non-Executive Directors, auditors, consultants, CISOs and academics. It is presented (Annex A) in the form of five overarching principles with relevant actions underneath each principle. The actions are framed in language that directors use, rather than being technical, and they go beyond being outcomes focused to provide a clearer expectation of directors. This will make it easier for directors in organisations of all sizes to understand which actions they should be taking, and why, so that they can better govern cyber risk.

The principles and actions of the Code have been drawn from best practice[1] and is intended to align with and complement existing industry and government resources, both in the UK and internationally. In particular, further guidance on implementation of these principles and actions, is provided within the NCSC's Cyber Security Toolkit for Boards and the two will work together to form a coherent set of guidance for boards, directors and their senior advisors.

Through this call for views, we want to test the design of the Code of Practice to determine whether the actions that directors should be taking to govern cyber risk are presented and explained in a way that is straightforward to understand and implement.

We also want to better understand what further guidance would help industry in order to be able to implement the code effectively. For example, the Australian Institute of Company Directors' Cyber Security Governance Principles makes use of a number of additional guidance pieces to form a suite of supports to assist organisations of all sizes. These include a 'checklist' for small and medium sized organisations and 'red flags' to help assist where an organisation might be erring.

Driving uptake

The proposed Code of Practice would be launched as a voluntary tool, that is, without its own statutory footing. However, the Code of Practice would support and align with a number of existing regulatory obligations. Whilst not sufficient on its own at driving the required improvements in cyber risk management at Board level, the government is exploring the Code's use in supporting regulators to understand how it can demonstrate compliance, including with the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS) regulations. The government will be working closely with these regulators and competent authorities, as well as broader sectoral regulators, to embed the Code in the existing regulatory landscape as and where it relates to cyber security and broader resilience.

However, as cyber risk now comprises a material risk to any business with a digital footprint, whether directly regulated or not, all organisations should adopt the Cyber Governance Code of Practice. To that end, the promotion of the Code, whether it is published through a governance or a cyber security agency, and the broader

[1] Existing guidance, standards, regulation and frameworks considered in the development of the draft Code of Practice include but were not limited to: the Corporate Governance Code; the FRC's Guidance on Audit Committees and Guidance on Risk Management, Internal Control and Related Financial and Business Reporting; NCSC's Cyber Assessment Framework, Cyber Security Toolkit for Boards, 10 Steps to Cyber Security, and Small Business Guide Actions: Cyber Security; ISO 27001; IASME Cyber Assurance; HMG's Security Policy Framework; the Defence Standard; PCI DSS; NIST's Cybersecurity Framework; CISA's Resources for Small and Midsized Businesses and Cyber Essentials Toolkit; ISACA's COBIT 5 for Risk and CMMI; AICD's Cyber Security Governance Principles; World Economic Forum's 6 Principles for Cyber Governance.

interventions outlined here to stimulate uptake, are all critical aspects of embedding it in common practice across the UK economy.

This call for views seeks input on where the Code may be best placed and promoted to ensure it reaches directors and forms a core aspect of their knowledge base on risk management in a digital age. As in other countries, such as the US and Australia, driving the required uptake will necessitate the Cyber Governance Code of Practice to be situated within existing guidance from a governance specific body, such as the Institute of Directors or the Chartered Governance Institute. Such a decision would need to be weighed against the confidence that government ownership would provide industry with when engaging with the Code, as well as the authority government ownership would provide with regards to embedding the Code in the existing regulatory landscape.

This call also seeks views on what role other bodies may play in the implementation and uptake of the Code. This includes, for example, considering trade, governance or sectoral organisations' role in promoting the Code, or the extent to which professional standards and training will impact the Code's uptake.

Finally, this call for views presents industry with the opportunity to provide the government with feedback on any potential barriers to implementation that should be considered, that are not already outlined in this document.

Assurance

As a form of driving uptake, the government is also seeking to explore the utility and risks of implementing either a self or independently assessed assurance process against the code. There are a number of potential use cases for an assurance against the Code. For example, shareholders, customers, insurance firms, or business partners can derive confidence in an organisation that has external assurance of their governance of cyber risks. This call seeks views on potential demand for an assurance mechanism to support the implementation of the Code, who might find value in an independently assured 'badge' and for what market communication and transparency purposes it would be used.

Equally, the call also seeks input on associated risks of assuring cyber governance. As with assurance against any other standard or framework, there are risks of the assurance becoming outdated, and with reliability of the assurance, particularly if self-assessed. Key considerations on this potential approach to driving uptake of the Code are sought in the questions contained within this call.

Annex A: Code of Practice

Cyber Governance Code of Practice				
Action 1	Action 2	Action 3	Action 4	Action 5
A: Risk management				
Ensure the most important digital processes, information and services critical to the ongoing operation of the business and achieving business objectives have been identified, prioritised and agreed.	Ensure that risk assessments are conducted regularly and mitigations account for changes in the internal, external and regulatory environments, which are more rapidly changing than in traditional risk areas.	Establish confidence in and take effective decisions on the level of cyber security risk that is acceptable to the organisation and how much will need to be managed to achieve the business objectives.	Ensure that cyber security risks are addressed as part of the organisation's broader enterprise risk management and internal control activities, and establish ownership of risks with relevant seniors beyond the CISO.	Gain assurance that supplier information is routinely assessed and reviewed commensurate to their level of risk, and that the organisation is resilient against cyber security risks associated with suppliers, stakeholders and business partners.
B: Cyber strategy				
Monitor and review the cyber resilience strategy in accordance with the level of accepted cyber risk, the business strategy, and in the context of legal and regulatory obligations.	Monitor and review the delivery of the cyber resilience strategy in line with current business risks and in the context of the changing risk environment.	Ensure appropriate resources and investment are allocated and used effectively to develop capabilities that manage cyber security threats and the associated business risks.		
C: People				
Sponsor communications on the importance of cyber resilience to the	Ensure there are clear cyber security policies that support a positive cyber security culture,	Take responsibility for the security of the organisation's data and digital assets by undertaking	Ensure the organisation has an effective cyber security training, education and	

business, based on the organisation's strategy.	and satisfy themselves that its culture is aligned with the cyber resilience strategy.	training to ensure cyber literacy and by keeping information and data they use safe.	awareness programme and metrics are in place to measure its effectiveness.	
D: Incident planning and response				
Ensure that the organisation has a plan to respond to and recover from a cyber incident impacting business critical processes, technology and services.	Ensure that there is regular, at least annual, testing of the plan and associated training, which involves relevant internal and external stakeholders. The plan should be reviewed based on lessons learned from the test and broader external incidents.	In the event of an incident, take responsibility for individual regulatory obligations, and support executives in critical decision making and external communications.	Ensure that a post incident review process is in place to incorporate lessons learned into future response and recovery plans.	
E: Assurance and oversight				
Establish a governance structure that aligns with the current governance structure of the organisation, including clear definition of roles and responsibilities, and ownership of cyber resilience at Executive and Non-Executive Director level.	Establish a regular monitoring process of the organisation's cyber resilience and review of respective mitigations and the cyber resilience strategy.	Establish regular two way dialogue with relevant senior executives, including but not limited to the CISO or relevant risk owner.	Establish formal reporting on at least a quarterly basis and have agreed a target range for each measurement on what is acceptable to the business.	Determine how internal assurance will be achieved and ensure the cyber resilience strategy is integrated across existing external and internal assurance mechanisms.

Annex B: Call for views survey questions

Section 1: Demographic questions

1. Are you responding as an individual or on behalf of an organisation?
    - Individual
    - Organisation

2. Which of the following statements best describes you?
    - Academic
    - Auditor
    - Company secretary
    - Cyber security professional
    - Executive Director
    - Non-Executive Director
    - Interested member of the public
    - Other [if selected, then a please specify text box appears]

3. [if organisation] How many people work for your organisation across the UK as a whole? Please estimate if you are unsure.
    - a. Under 10
    - b. 10–49
    - c. 50–249
    - d. 250–499
    - e. 500-999
    - f. 1,000 or more
    - g. Not sure

4. [if individual] Where are you based?
    - England
    - Scotland
    - Wales
    - Northern Ireland
    - Europe (excluding England, Scotland, Wales and Northern Ireland)
    - North America
    - South America
    - Africa
    - Asia
    - Oceania (Australia and surrounding countries)
    - Other [if selected, then a please specify text box appears]

5. [if organisation] Where is your organisation headquartered?
    - England
    - Scotland
    - Wales
    - Northern Ireland
    - Europe (excluding England, Scotland, Wales and Northern Ireland)
    - North America
    - South America
    - Africa
    - Asia
    - Oceania (Australia and surrounding countries)
    - Other [if selected, then a please specify text box appears]

6. Are you happy for the Department for Science, Innovation and Technology to contact you to discuss your response to this call for views further?
    - Yes
    - No

7. [If yes] Please provide us with a contact name, organisation (if relevant) and email address.

Section 2: Design questions

In this section, we would like to get your views on the five principles in the Code of Practice that was co-designed with NCSC and industry experts (Annex A). We will ask you about each principle in turn and whether any other principles should be considered.

A: Risk management

8. Do you support the inclusion of this principle within the Code of Practice?
    - Yes
    - No
    - Don't know

B: Cyber strategy

9. Do you support the inclusion of this principle within the Code of Practice?

- Yes
- No
- Don’t know

C: People

10. Do you support the inclusion of this principle within the Code of Practice?
    - Yes
    - No
    - Don’t know

D: Incident planning and response

11. Do you support the inclusion of this principle within the Code of Practice?
    - Yes
    - No
    - Don’t know

E: Assurance and oversight

12. Do you support the inclusion of this principle within the Code of Practice?
    - Yes
    - No
    - Don’t know

13. Are there any principles missing from the current version of the Code of Practice?
    - Yes
    - No
    - Don’t know

14. [if answered yes] Please set out any new principles that you think should be included and explain why. (1800 characters)

15. Are there any other actions missing from the current version of the Code of Practice?
    - Yes
    - No
    - Don’t know

16. [if answered yes] Please set out any new actions that you think should be included and explain why. (1800 characters)

17. What relevant guidance should be referenced in the publication of the Code of Practice to support Directors in taking the actions set out in the Code? (1800 characters)

18. What tools, such as 'green flags' i.e. Indicators of good practice, checklists, etc. should be included within the publication or issued alongside the Code of Practice to support Directors in taking the actions set out in the Code? (1800 characters)

Section 3: Driving uptake questions

19. Where should the code be published?
    Please select all that apply. [Multi-code]
    - Institute of Directors website
    - FRC website
    - NCSC website
    - Gov.uk
    - Other - industry website [free text to fill out]
    - Other - government website [free text to fill out]

20. With whom should government work to promote the Code to ensure it reaches directors and those in roles with responsibility for organisational governance? (1800 characters)

21. What products or services (including Director training programmes, existing guidance, accreditation products, etc.) could the Code be incorporated within to support its uptake with directors? (1800 characters)

22. What organisations or professions could best assist in driving uptake of the Code with directors?
    Please select all that apply. [Multi-code]
    - Asset Management Companies
    - Auditors
    - CISOs
    - Company Secretaries
    - Insurers
    - Investors
    - Lawyers
    - Regulators
    - Risk / Audit Committees

- Shareholders
- Other [please specify]

23. [if answered ‘Other’] Please set out any other market stakeholders not included and explain why. (1800 characters)

Section 4: Assurance questions

24. [if organisation] Would your organisation be interested in receiving external assurance of your organisation’s compliance with the Code?

- Yes
- No
- I don’t know
- Not applicable

25. [If organisation] Please explain your answer. (1800 characters)

26. [If answered yes] If yes, what would encourage you to gain assurance of the code?
Please select all that apply. [Multi-code]

- Improving overall cyber resilience
- Assist with regulatory compliance, including the UK GDPR and NIS
- Matching existing standards held by competition in your sector
- Compliance with supply chain requirements
- Providing reassurance externally and internally e.g to customers and shareholders
- Other [please specify]

27. What type of external assurance should be used to demonstrate compliance with the code?
Please select all that apply. [Multi-code]

- Self assessment, with external review of assessment (not audit of governance practices)
- Spot checks
- Independent audit
- Other [please specify]

28. Which organisations or professions would place value on other organisations having received assurance against the code? Please select all that apply. [Multi-code]
    - Asset Management Companies
    - Auditors
    - CISOs
    - Company Secretaries

- Insurers
- Investors
- Lawyers
- Regulators
- Risk / Audit Committees
- Shareholders
- None
- Other

29. [if answered ‘Other’] Please set out any other market stakeholders not included and explain why. (1800 characters)

Section 5: Barriers to implementation

30. What barriers may exist to effective uptake of the Code?
    Please select all that apply. [Multi-code]
    - Cyber resilience not being a priority of directors (of organisations of all sizes)
    - Existing guidance is already effective [if so, state which guidance]
    - Viewed as a cyber technical piece of guidance
    - Actions are not positioned at director-level activities
    - Lack of reach into directors of small and medium sized organisations
    - Other [please specify]

Section 6: Conclusion

31. Thank you for taking the time to complete the survey. We appreciate your time. Is there any other feedback that you wish to share?
    - Yes
    - No

32. [If yes] Please set out your additional feedback in the box below. (2500 characters)