Department for
Science, Innovation
& Technology

Cyber Governance Code of Practice: government response to the call for views

CP 1260

Cyber Governance Code of Practice: government response to the call for views

Presented to Parliament
by the Secretary of State for Science, Innovation and Technology
by Command of His Majesty

January 2025

CP 1260

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at cybergovernance@dsit.gov.uk

ISBN 978-1-5286-5412-8

E03270244 01/25

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

Contents

Ministerial foreword

This government is committed to supporting businesses and driving UK economic growth. As Secretary of State for the Department for Science, Innovation and Technology (DSIT), it is one of my top priorities to ensure that new and existing technologies are safely developed and deployed across the UK with the benefits accessible to all. Businesses and organisations are becoming increasingly reliant on digital technologies. This is helping maximise innovation, efficiency and growth across the economy.

The growth of digitisation and the opportunities that it unlocks also presents an increasing and evolving cyber risk. 50% of UK businesses experienced some form of cyber security breach or attack in the previous 12 months[1]. These can lead to adverse impacts such as a loss of income from being unable to operate due to losing access to systems, or reputational damage caused by the loss of customer data.

It is clear that the UK needs to take a stronger approach to improve our cyber resilience and ensure that organisations across the economy are appropriately prepared for cyber incidents. The Cyber Security Breaches Survey 2024 highlighted that cyber security is a high priority for senior management in most organisations, but a lack of knowledge, training and time is preventing boards from engaging more.

The Cyber Governance Code of Practice, developed by DSIT in collaboration with the National Cyber Security Centre and industry, has been designed specifically to support this need. It formalises the government's expectations regarding an organisation's governance of cyber security and sets out clear actions that directors, and non-executive directors need to take to meet their responsibilities in managing cyber risk.

The draft code was published as part of a call for views earlier this year. I would like to thank everyone who engaged with it and provided responses. I would also like to thank all the organisations that either hosted, or participated in, one of the many events, workshops, and webinars with DSIT officials during the call for views period. This work garnered significant interest and opinion from a range of stakeholders across the UK economy and society, reflecting the importance of this issue and the support for action. We have listened to what you have had to say and have made a

[1] UK Cyber Security Breaches Survey 2024

number of commitments to improve the code of practice and support its implementation. These are outlined in this Government response.

The cyber risk facing the UK is broad and complex, and our response needs to be comprehensive. The Cyber Governance Code of Practice is just one element of what this government is doing to drive up cyber security across the economy. We have committed to improving the cyber security of our critical national infrastructure through the Cyber Security and Resilience Bill and are also taking a range of actions to help increase the cyber resilience of the wider economy and society and ensure the safe deployment of technologies. This includes working to close the skills gap by continuing investment in our cyber skills programmes, such as CyberFirst; driving uptake of important baseline schemes such as Cyber Essentials; introducing further Codes of Practice on software security, and the cyber security of AI; as well as existing work on product security; through the Product Security and Telecommunications Infrastructure Act 2022 and the Code of Practice for app store operators and developers.

With your continuing engagement and support for this Cyber Governance Code of Practice, and the wider programme of initiatives, we can significantly strengthen the UK's cyber resilience and make it a world leader for secure digital innovation and investment.

The Rt Hon Peter Kyle MP

Secretary of State

Department for Science, Innovation and Technology

1. Executive summary

Digital technologies are now firmly embedded within the vast majority of businesses and organisations across the UK, regardless of size. For most, critical business operations, such as payroll and invoicing, could not happen without digital technologies. However, directors and boards often have little to no meaningful oversight over how these technologies are used and managed, despite the business critical risks if something happened to them.

Cyber incidents can lead to major impacts on businesses and organisations whether that is direct loss of income due to disruption of services, damage to customer trust following theft of personal data or intellectual property, or costly remedial action following a ransomware attack. To further complicate matters, businesses and organisations can be heavily impacted even where they are not directly attacked. This occurred when organisations had their staff data breached due to an attack on the MOVEit file transfer software in June 2023. Incidents can affect businesses and organisations of all sizes, as demonstrated in July 2024, when a global IT outage disrupted services to customers for almost ten hours. These incidents clearly highlight the need for all businesses and organisations to understand and manage digital dependencies and risks across core services and supply chains.

Good cyber governance at the board level sets the tone for building resilience to a wide range of cyber risks across the organisation, while poor governance increases barriers to effective cyber risk management and slows down critical decision-making. The Cyber Security Breaches Survey 2024 shows that boards and senior leaders still struggle to engage in cyber issues due to lack of understanding, training and time, and just 30% of all UK businesses and charities have board members or trustees with explicit responsibility for cyber security.

Instead, these decisions are often delegated to technical experts, and digital and cyber issues are considered separately to wider business risk management. Challenges in communication between technical experts and directors further widen this gap and can lead to material impacts on budget allocations, the business's overall risk profile, and critical gaps in accountability.

To help address these issues and support directors in fulfilling their responsibilities in managing cyber concerns alongside wider business issues, DSIT is developing a Cyber Governance Code of Practice. This is in line with DSIT's commitment to ensure that new and existing technologies are deployed safely across the UK to enable more businesses and organisations to make the most of the opportunities they bring.

The code, which has been co-designed with technical experts from the NCSC and a range of governance experts across industry, focuses on the actions that leaders should take or should ensure are taken to govern cyber risk effectively within their organisation.

The proposed code of practice was published as part of a call for views in January 2024. This call for views was an invitation for any industry stakeholders or other interested party to provide feedback on three key areas:

- the design of the 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.

During the period of the call for views, DSIT conducted extensive engagement to discuss the issues in more detail with a range of industry and academic stakeholders including trade bodies, professional associations, company directors and non-executive director networks. In total, DSIT reached over 1,700 stakeholders at 20 events. 160 survey responses were analysed. Data from both the written survey responses and the engagements has been analysed to inform how the code of practice is taken forward.

This document provides an overview of the responses to the call for views and key themes that emerged, as well as stating the government's response to the feedback. This is structured around five key themes from the responses, as follows:

A. There was overall support for the aims and design of the code, with a range of suggestions for further additions;
B. Most respondents were in favour of an assurance scheme, however support depended on the design of the scheme;
C. A large number of respondents commented on the wide target audience of the code and the implications of this on promoting uptake;
D. Many respondents requested further clarity over links with other standards, guidance and resources; and
E. There was interest in government working with a wide range of stakeholders to promote uptake of the code.

The document ends with an outline of next steps including a commitment to publish the Cyber Governance Code of Practice in early 2025.

2. Background

DSIT is committed to ensuring that new and existing technologies are deployed safely across the UK. This is to enable businesses and organisations to make the most of the varied opportunities they bring. This will include the introduction of a Cyber Security and Resilience Bill to better protect the UK's critical systems. However, more must be done to ensure that all businesses and organisations across the wider economy are able to manage their cyber risks and implement new technologies with confidence.

Cyber security is seen as a high priority by senior management in 75% of businesses and 63% of charities[2]. The Chartered Institute of Internal Auditors also identified cyber security as the highest rated risk for organisations currently and the top risk that leaders expect their organisations to be facing in the next three years[3]. The Information Commissioner's Office (ICO) has called on organisations to boost their cyber security amid a growing number of cyber security breaches[4], to ensure that organisations fulfil their obligations under General Data Protection Regulation (UK GDPR) to protect personal information. The Financial Reporting Council (FRC) has also taken further steps to raise the profile of cyber security risk management in its Corporate Governance Code Guidance[5], which sets out the importance of the board governing cyber risk.

However, relatively few businesses and organisations have clear lines of accountability to ensure cyber security is governed adequately. The Cyber Security Breaches Survey 2024 shows that only 30% of UK businesses and charities have board members or trustees with explicit responsibility for cyber security as part of their job role. Boards are prevented from engaging more in cyber security due to a lack of knowledge, training and time[6]. Evidence from the Department for Digital, Culture, Media & Sport's (DCMS) 2020 call for evidence on cyber security incentives and regulations shows a clear demand from industry for clearer direction on "what good looks like". This is particularly the case for directors who do not have a technical background in cyber[7].

The aim of the Cyber Governance Code of Practice is to address these issues by supporting directors and board members to understand what they should be doing as a minimum to oversee cyber risk management. While there is no one size fits all approach, there are some common fundamental actions that all directors and their organisations should take. This code is intended to provide a clear set of actions which are framed in language that directors use. The code is intended to make clear the links between cyber and other business risks and it will formalise the government's expectations of directors in governing cyber risk.

---

[2] 2024 Cyber Security Breaches Survey

[3] 2024 Risk in Focus: https://charterediia.org/media/sh4agazt/risk-in-focus-2025.pdf

[4] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/05/organisations-must-do-more-to-combat-the-growing-threat-of-cyber-attacks/

[5] https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/corporate-governance-code-guidance/

[6] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

[7] https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence/cyber-security-incentives-regulation-review-summary-of-responses-to-the-call-for-evidence#:~:text=Findings%20from%20this%20section%20of,lack%20of%20commercial%20rationale%20all

DSIT is also exploring how the code can be used to support regulators to understand how it can assist with regulatory compliance, including with UK GDPR.

The draft code of practice comprises five principles which are each underpinned by between three to five actions. These principles are risk management, cyber strategy, people, incident planning and response, and assurance and oversight. The code has been designed to complement the NCSC's Cyber Security Toolkit for Boards. While the code sets out what directors should be doing to govern cyber risk, the Toolkit provides further detail on how directors should undertake the activities outlined in the code and why. It is our expectation that the code and the toolkit will work together to form a coherent set of guidance for directors and boards.

The Cyber Governance Code of Practice also forms an integral part of a wider package of codes of practice being developed by DSIT[8]. This code of practice will act as a foundational code that has a particular focus on medium and large organisations across all sectors but can be used by all organisations. Other draft codes of practice including the software vendors and AI, which were published for consultation in May, are relevant to specific sectors or areas of technology. These are in addition to the previously published App Stores and Consumer IoT codes of practice. Organisations that are in scope of these codes would also be expected to follow the governance code. The collection of codes of practice are part of the Government's broader approach to improve baseline cyber security practices and cyber resilience across the UK. DSIT has developed a modular approach to implementing codes of practice to help organisations understand how they interact and which codes are relevant to them. Details of this approach can be found here.

3. Methodology

The call for views was open from January 22 to March 18, 2024. The survey was open to the public and responses were received from individuals and organisations. Respondents were invited to participate via an online survey or to submit responses by email.

The call for views asked respondents 32 questions on the draft code of practice, including both closed and open questions. Respondents did not have to answer every question.

160 responses were included in the analysis. This was made up of 140 online responses, and 20 email responses. For inclusion in the analysis, respondents had to have answered questions from at least one of the main sections (Design, Uptake, Assurance) or submitted a response in the 'additional feedback' question. Responses were excluded from the analysis if they did not provide any answers in

[8] https://www.gov.uk/government/collections/cyber-security-codes-of-practice#:~:text=Codes%20of%20Practice%20have%20been,a%20given%20set%20of%20risks

these sections (i.e. only answered the demographics questions). Some responses were also excluded because they were duplicates.

For open response questions, every response was reviewed, and while not every point that was made by each respondent can be reflected, responses were coded to identify common themes.

A Privacy Notice was provided containing information for participants on their rights and how their responses will be used. All personally identifiable information has been removed from the analysis.

4. Key themes and government response

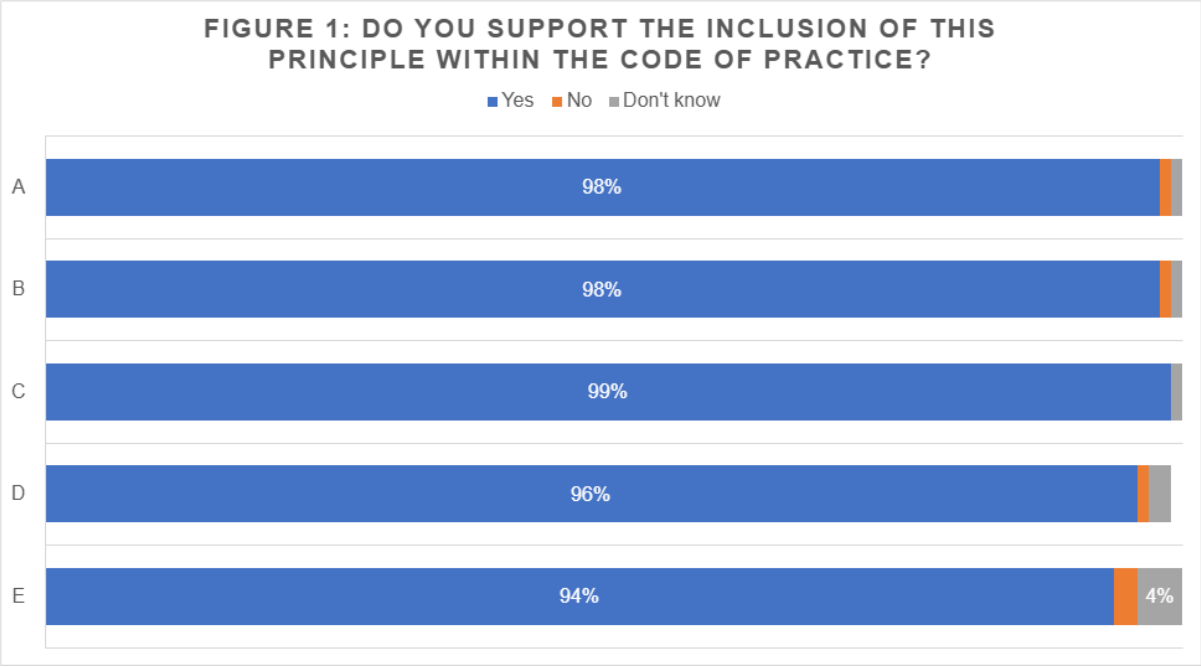
a. Overall support for the code's design, with some further proposals.

One of the main aims of the call for views was to seek feedback on the design of the code of practice and the extent of the support for the different elements within the code.

Analysis of responses

The responses to the call for views showed that there was overall support for the design of the code. As shown in Figure 1, the majority of respondents agreed that the proposed principles should be included in the code (94% or more support each principle).

Figure 1: Do you support the inclusion of this principle within the code of practice?



Unlabelled bars are less than 2%.
Base sizes: A: 141, B: 141, C: 141, D: 141, E: 142

The call for views also asked if any principles are missing from the code. 39% said there were principles missing from the code, whilst 33% said there were no principles missing. A further question asked if any actions were missing. 40% of respondents said there were actions missing from the code, whilst 38% said there were not. Other respondents said they didn't know (28% for principles, 23% for actions).

Qualitative feedback from respondents included suggestions for various additional principles. One key theme was the suggested addition of a technical measures principle, covering areas such as the maintenance and management of technical and IT controls, and (existing and emerging) technologies. There was also interest in guidance for boards and directors on how their involvement can support this, which respondents perceived as fundamental to the problems faced with cyber security. Another common suggestion was for an additional principle covering supply chains and third parties, including for software. Respondents highlighted that this is an area where organisations currently fail to review and manage risks.

Qualitative feedback on additional actions mostly related to non-technical measures to promote good cyber governance, for example internal controls, regulatory compliance and naming responsible individuals for cyber governance.

Overall, the call for views responses showed that there was strong support for the draft code's design, as shown above in Figure 1.

Government response

DSIT recognises the strong positive feedback on the inclusion of each of the five proposed principles, with 94% or more of respondents agreeing with the inclusion of each principle. Feedback on which further principles or actions would be required was mixed and inconclusive.

DSIT will not make any major changes to the design of the code of practice before it is published. DSIT will, however, work with NCSC and industry stakeholders to make minor changes to the wording to provide better clarity and ensure the terminology is correctly pitched for the intended audience. DSIT will also assess the uptake and impact of the code after publication and will work with stakeholders to review and, if necessary, update the code periodically.

DSIT recognises the request by some for the addition of further principles and actions, particularly related to technical measures. DSIT's position is that it would not be appropriate to include specific technical measures to the code of practice for several reasons. These include the broad target audience of the code across multiple sectors, the intention for it to be used by non-cyber specialists, and the rate at which technology and the technical measures required evolves. DSIT will,

however, signpost relevant NCSC guidance in the materials accompanying the code when published.

b. Most respondents in favour of an assurance scheme, subject to its design and benefits

Seeking feedback on assurance against the code of practice formed one of the three main topics of the call for views. When discussing the proposed code, assurance is a topic that often prompts conflicting views from different industry stakeholders.

Assurance schemes can help organisations to demonstrate that they meet a certain piece of guidance or a set of standards. These can be used to demonstrate compliance to potential customers, streamline supplier management processes, and increase the incentives to follow good cyber security practices.

However, NCSC[9] and respondents to previous call for views[10] have expressed caution about over-reliance on assurance schemes. This could create false confidence and reduce the incentives to take other cyber security action if the limitations of an assurance scheme are not fully understood. This could happen, for example, if a stakeholder doesn't realise a certification only applies to part of an organisation rather than the whole or a certification has not been renewed when it should have been.

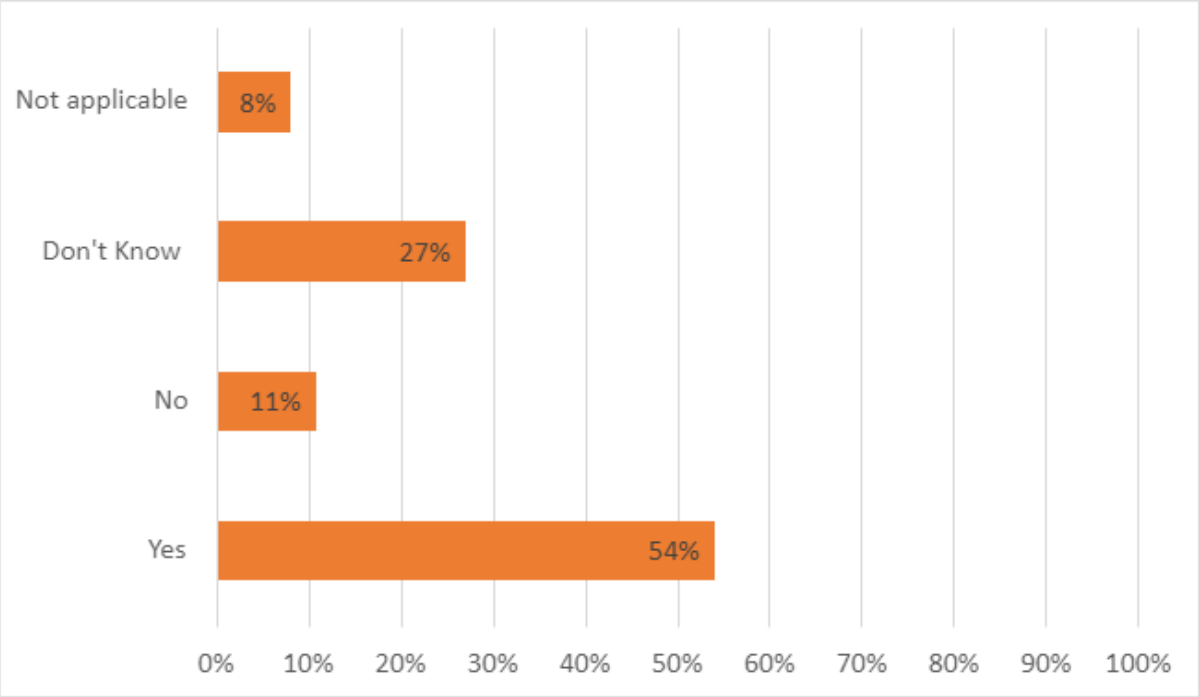
In the call for views, respondents were asked for their views on whether their organisation would be interested in receiving external assurance against the code, the reasons for this, and the type of external assurance that would be of greatest interest.

Analysis of responses

The call for views showed that there was interest in an assurance scheme, however support would depend on its design and perceived benefits to organisations. Around half of respondents (54%) reported that their organisation would be interested in receiving external assurance of compliance with the code (Figure 2.1).

[9] NCSC Cyber Security Toolkit for Boards
[10] Government response to the call for views on software resilience and security for businesses and organisations

Figure 2.1: Would your organisation be interested in receiving external assurance of your organisation's compliance with the code?



Base: 74

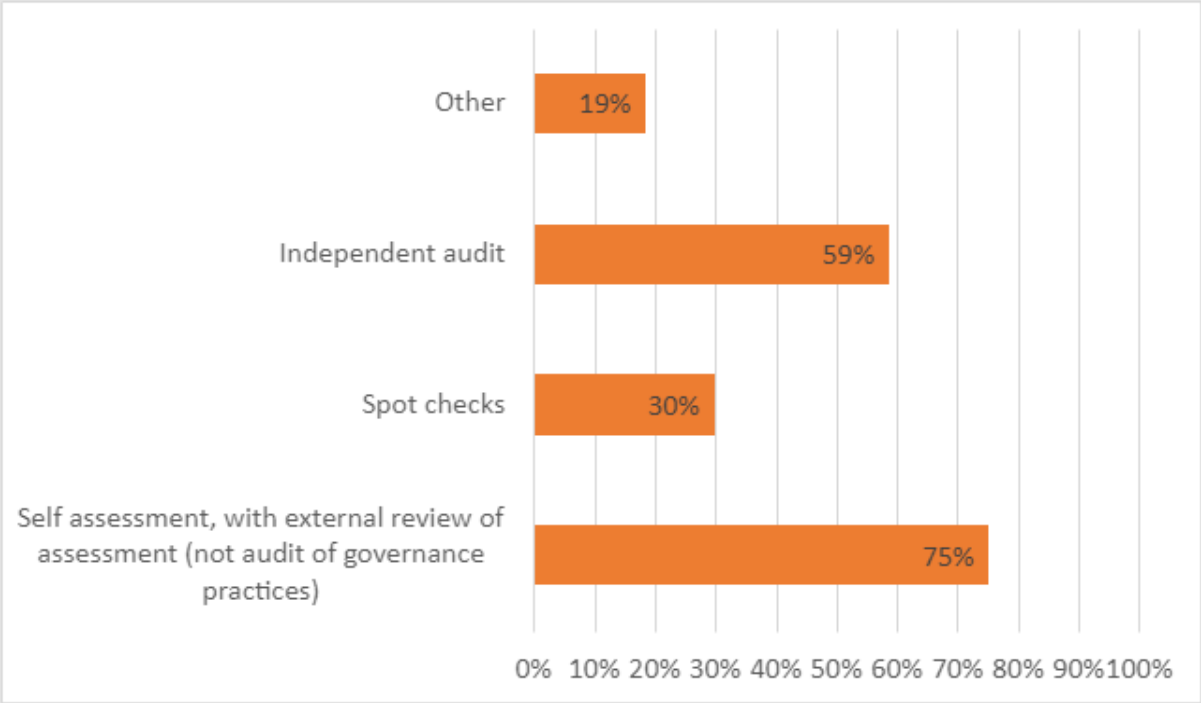
Qualitative feedback showed that those respondents who were interested in external assurance tended to think it would demonstrate overall compliance and resilience to external stakeholders, notably customers, suppliers, and other organisations. Other benefits of external assurance of the code identified by respondents were that it would offer a competitive advantage and allow for better understanding of risks internally and provide assurance for internal stakeholders (e.g. the board).

Respondents who were not in favour of external assurance (11%) tended to say that it would lack further benefit to their organisation as they already have existing accreditations. Some also stated that it would be too burdensome, and particularly for smaller organisations.

As shown in Figure 2.1, 27% of respondents also said that they ‘don’t know’ if their organisation would be interested in external assurance. Qualitative feedback suggested that several of these respondents would only be interested in external assurance depending on the costs and associated benefits. Furthermore, some of these respondents were only interested in external assurance in certain forms, with several saying that it would depend on the framework of the assurance, and who provides it. There was little consensus on these areas. For example, there was disagreement between responses on whether it should be a government department/arms-length body or a private firm who should deliver an assurance scheme.

There was strong interest in external assurance to the code involving a self-assessment with an external review of assessment, and some interest in an independent audit, as shown in Figure 2.2. It should be noted that respondents often selected both. This might indicate interest in a tiered external assurance scheme and reflect calls for the code to be sensitive to different types of organisations. Several respondents who selected 'other' when asked about what type of external assurance should be used explicitly mentioned interest in a tiered accreditation scheme akin to Cyber Essentials and Cyber Essentials Plus.

Figure 2.2: What type of external assurance should be used to demonstrate compliance with the code? Please select all that apply.



Base: 97

Overall, the call for views highlighted the importance of the design of an external assurance scheme. While some areas on design and benefits lacked consensus, there was stronger indication of an interest in external assurance in the form of self-assessment and independent audit.

Government response

Responses to the call for views show that there is a high level of interest in a potential assurance scheme to accompany the code of practice. However, there are considerable challenges to establishing an effective assurance scheme that would be useful to organisations and their stakeholders. The government will take care to ensure that a new assurance scheme does not create undue burden for organisations nor create perverse incentives for weaker security behaviours. For example, a poorly designed assurance scheme could encourage an organisation to

opt for “quick fixes” to achieve certification rather than considering what is appropriate to the organisation.

DSIT will therefore publish the code of practice without an accompanying assurance scheme in early 2025. DSIT will, however, work closely with key stakeholders to further explore the possibility of establishing an accompanying assurance scheme at a later point. This is to ensure that the benefits of a voluntary code of practice can be realised earlier without compromising the process of designing a good assurance scheme.

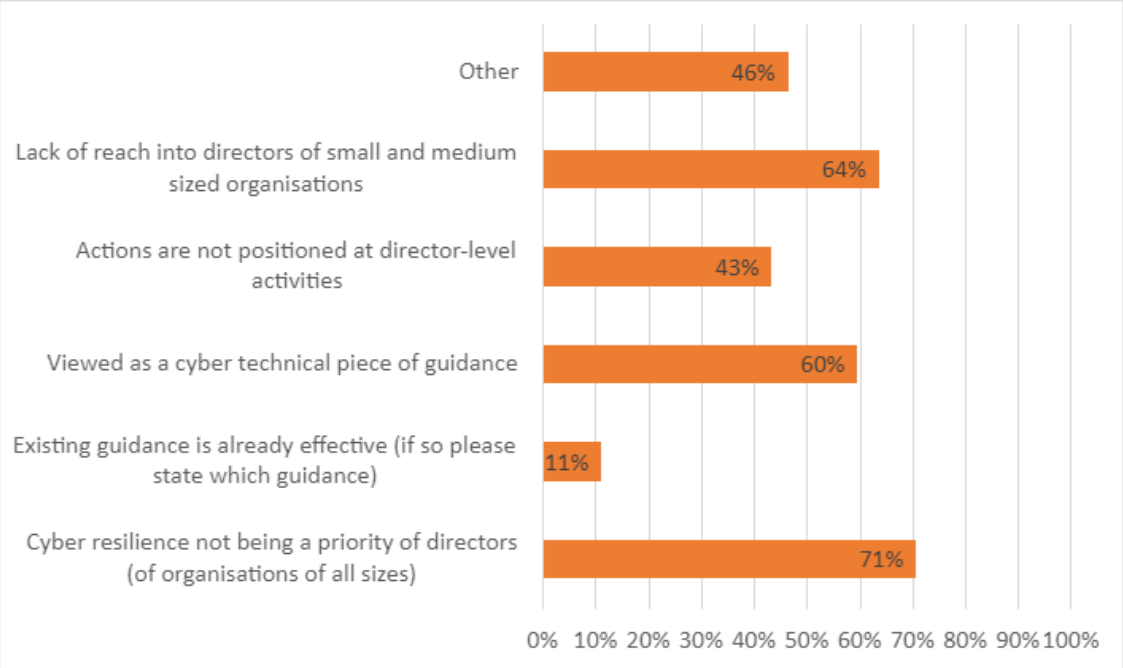
c. Scope of the code and its implications on uptake

The cyber governance code of practice was designed to be applicable to organisations of all sizes and in all sectors. The actions included in the code are intended to be those that all organisations should do, while recognising that some organisations may need to do more depending on their risk profile and nature of the organisation. However, the scope of the code and its applicability to different types of organisations, particularly small organisations, was a key theme raised by respondents.

Analysis of responses

The call for views prompted feedback on the scope of the code, with an indication from many respondents that smaller organisations would struggle to implement the guidance. When asked about barriers to effective uptake, the top three barriers selected were that cyber resilience is not a priority of directors of organisations of all sizes (71%), that there is a lack of reach into directors of small and medium sized organisations (64%) and that the code is viewed as a cyber technical piece of guidance (60%) (Figure 3).

Figure 3: What barriers exist to effective uptake of the code? Please select all that apply.



Base: 99

Qualitative responses reinforced this feedback. While respondents expressed general support for the code and government work on cyber governance, many gave at least one caveat to their support linked to the code's scope and uptake. Most prominently, respondents felt that different sizes of organisations have various needs to which the code is not currently adapted (particularly smaller organisations). In some qualitative responses, respondents also stated that external assurance would be particularly costly for smaller organisations, making it harder to drive uptake. Overall, which organisations are in scope of the code and any potential external assurance emerged as a key area of interest, and in some cases criticism of the code. However, most suggested that adapting the current draft of the code or having variations of the code would be sufficient for different organisation types.

Government response

Following this feedback, DSIT will clarify that the Cyber Governance Code of Practice will be targeted primarily at medium and large businesses and organisations. The terminology used in the code will be tailored toward these organisations. Government expectations are that all medium or larger businesses and organisations (50 employees or more) should be able to implement the code.

It should be noted, however, that many small businesses (fewer than 50 employees) play a critical role in the cyber security of wider digital supply chains. This could be due to the sensitivity of data they process on behalf of other organisations or because they provide a critical service to an organisation with a particularly high risk

profile, such as a critical national infrastructure operator. In such cases, the small business should consider using the code of practice to inform their cyber security governance practices. They may wish to adapt the actions under each principle to their circumstances while aiming to achieve the same outcomes.

Other small businesses and organisations may wish to do similar depending on their cyber maturity and risk profile. DSIT recommends that small businesses and organisations refer to the NCSC website for further guidance that is tailored specifically to these audiences. DSIT is continuing to work with NCSC to explore how to support small businesses and organisations in implementing good cyber security, including the themes covered by the code of practice.

Organisations that have a high risk profile, such as critical national infrastructure owners and operators, should also use the code of practice to inform discussions and agreements with their suppliers of all sizes.

d. Clarity over links with other standards, guidance and other resources

In the call for views, respondents were asked for suggestions for how to promote uptake of the code of practice, particularly in terms of links with other organisations and their products or services. As part of this, respondents emphasised the need for greater clarity about how the code relates to this wider context of industry standards and government policy, both domestic and international.

Analysis of responses

Respondents to the call for views showed strong interest in gaining further information on how the code links to other standards, guidance and resources. In particular, there was interest in more information on how the code 'maps' against existing work for clarity and consistency, and for the perceived benefit to its uptake.

The call for views survey included several questions about which relevant guidance should be referenced in the publication of the code, any tools that should be issued alongside the code/its publication, and which products and services the code should be incorporated within. Feedback strongly indicated that the code should be linked to existing government guidance and legislation, particularly NCSC guidance. Additionally, respondents referred to various international or sector-specific examples of guidance and regulation (e.g., NIST, NIS2, FCA guidance). It was also suggested that the code should be incorporated in existing training programmes (especially board and director targeted training) and several respondents identified that the code could be incorporated within insurance questionnaires. Notably respondents often highlighted the potential to ‘map’ the code against other resources, guidance and standards, to show organisations where overlaps are and to create consistent approaches to cyber governance.

There was also some interest in new guidance and resources (e.g. indicators of good practice or maturity ratings specifically made around the code). This feedback tended to emphasise that new guidance, standards and tools should be aimed specifically at directors (e.g. with plain language explaining technical aspects) and/or that it should be derived from, or cohere with, existing guidance.

In general, the call for views showed there is interest in ensuring that the code is joined up and contextualised for organisations with other guidance and resources, both domestic and international.

Government response

At the time of publishing the code of practice, government will provide additional information on how the code relates to key international and industry standards and guidance. DSIT will work with industry and international stakeholders to explore the possibility of conducting formal mapping between these and the Cyber Governance Code of Practice. The code will also be mapped to the NCSC Board Toolkit, which will help Board members and senior leaders to understand how the requirements of the code can be implemented.

e. Interest in government working with a wide range of stakeholders to promote uptake of the code

To promote uptake of the code of practice, government will engage with a variety of stakeholders. This would be to outline both why boards and directors should take further action on cyber governance and why adopting the code of practice is the best course of action. As part of the call for views, DSIT asked for suggestions for who they should work with to promote the code.

Analysis of responses

The call for views showed that there was interest in government engaging with a wide range of stakeholders in encouraging uptake of the code.

The survey asked respondents which organisations or professions could best assist in driving uptake of the code with directors. The most commonly selected responses were risk/audit committees, CISOs, regulators and auditors – each of these were selected by 60% or more of respondents (Table 1).

Table 1: What organisations or professions could best assist in driving uptake of the code with directors? Please select all that apply

Organisation/profession	Number	%
Asset management companies	27	27%
Auditors	64	63%
CISOs	72	71%
Company secretaries	45	45%
Insurers	60	59%
Investors	44	44%
Lawyers	35	35%
Regulators	68	67%
Risk/audit committees	76	75%
Shareholders	40	40%
Other	36	36%

Base: 101

Qualitative feedback showed that respondents particularly encouraged the government to work with professional, trade and industry bodies (e.g. Institute of Directors, the Federation of Small Businesses, Confederation of British Industry, Chambers of Commerce) and board networks.

Many respondents also suggested that external groups (i.e. those who could hold organisations accountable to the code) should be involved in the promotion of the code, with respondents most commonly mentioning regulators, auditors, accountants, insurers and lawyers as key professions and organisations. Various types of cyber and IT-specific organisations were also mentioned by some respondents (e.g. NCSC, cyber training providers, and Warning, Advice and Reporting Points (WARPs)).

Overall, respondents tended to express interest in government working with more than one of these types of organisations and professions, suggesting that there is interest in the government having broad engagement to promote the code.

Government response

DSIT will work closely with a wide range of stakeholders throughout implementation of the code of practice to promote great uptake. DSIT will particularly focus on engaging with professional, trade and industry bodies and board networks. DSIT will also work with groups who could hold organisations accountable to the code such as regulators, auditors, accountants, insurers and lawyers. Working with these groups will be particularly important to promoting uptake of the code once it is published.

DSIT will also continue to work with its existing network of cyber security professionals to test the design and assess the impact of the code's implementation. This will be important to ensure that the code adequately accounts for current and future cyber threats as the nature of cyber security evolves over time.

f. Other issues raised

Some calls for legislation

As outlined in the call for views, the intention is for the code of practice to be launched as a voluntary tool, that is, without its own statutory footing. Respondents to the call for views were not directly asked for their views on making adherence to the code a legal obligation for certain organisations although several raised it in their response to other questions, particularly those related to assurance and driving uptake.

Analysis of responses

There was some feedback from the open text questions in the call for views that called for legislation on cyber governance. Although this was a view amongst a minority of respondents, it was a recurring theme in several areas of qualitative feedback.

For example, when asked about which products or services the code should be incorporated within, several respondents suggested that it should be integrated into legislation or regulation. Of these responses, most referred to existing legislation (e.g. the Data Protection Act and NIS), however some also suggested the code should be incorporated in new cyber and technology regulations.

Calls for legislation were also noted in the additional feedback received, where there was some support for making the code mandatory or introducing regulations around it.

Overall, there was some interest in legislation on cyber governance to be noted from the call for views, although this was from a minority of respondents.

Government response

DSIT will publish the code of practice as a voluntary tool in early 2025. The government will monitor uptake of the code and evaluate its effectiveness in driving improvements in how cyber risk is governed. DSIT will continue to explore options for how the code could be used to assist with regulatory compliance, including UK GDPR. If uptake of the code is limited and there are not sufficient improvements in how cyber risk is governed, DSIT will look into options for firmer levers to promote greater uptake. This may include the future introduction of legislation and/or the utilisation of public procurement requirements.

5. Next steps

Working closely with NCSC, DSIT will make minor edits to the Cyber Governance Code of Practice before publishing it in early 2025.

DSIT and NCSC will develop materials to support implementation of the code and will work closely with industry stakeholders to promote uptake. These industry stakeholders will include professional, trade and industry bodies and board networks as well as groups who could hold organisations accountable to the code.

DSIT will seek to work with industry to develop a public pledge that will encourage uptake of the code by celebrating key partners who are implementing the code and seeking to drive uptake within their sectors.

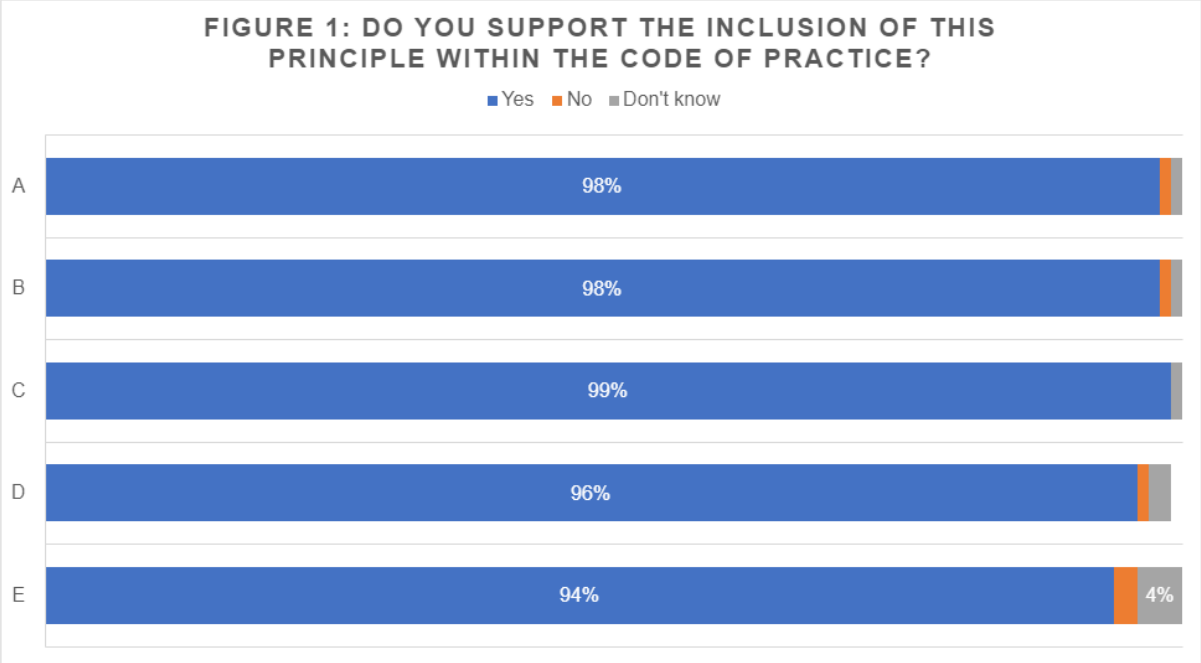
DSIT and NCSC will work to provide clarity on interactions between the Cyber Governance Code of Practice and other government policy, standards, guidance and resources. This includes the upcoming Cyber Security and Resilience Bill.

DSIT will work with NCSC and industry stakeholders to monitor uptake and implementation of the code of practice. DSIT will adjust and update policy as needed following these findings and as the cyber security and technology landscapes evolve over time.

Annex A – closed question survey findings and charts

This annex contains charts and quantitative data from responses to the closed questions in the call for views survey. They are provided in this annex to demonstrate full transparency of the quantitative data.

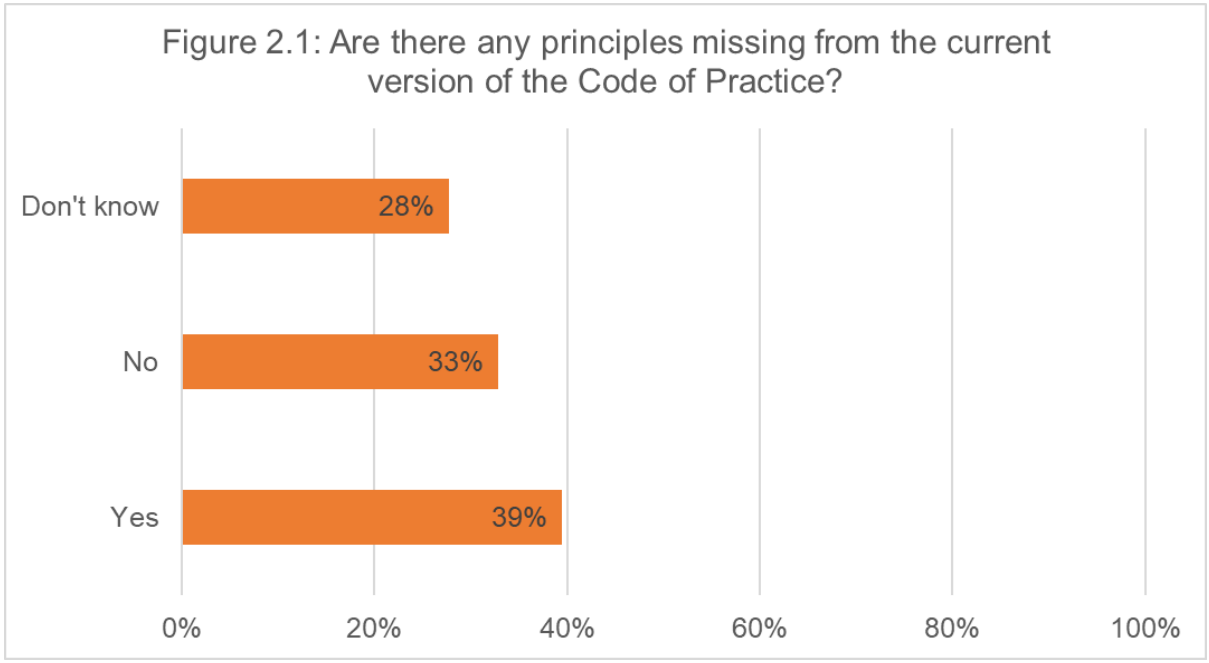
Q8-12: Do you support the inclusion of this principle within the Code of Practice?



Base sizes: A: 141, B: 141, C: 141, D: 141, E: 142

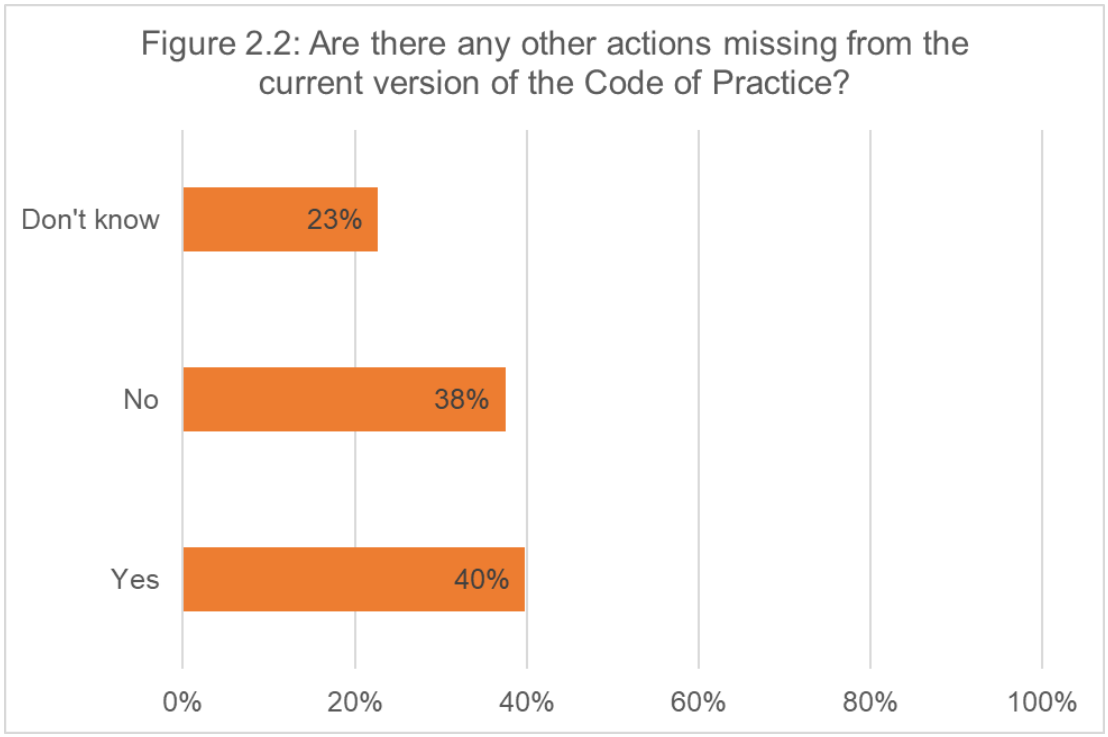
Unlabelled bars are less than 2%.

Q13: Are there any principles missing from the current version of the Code of Practice?



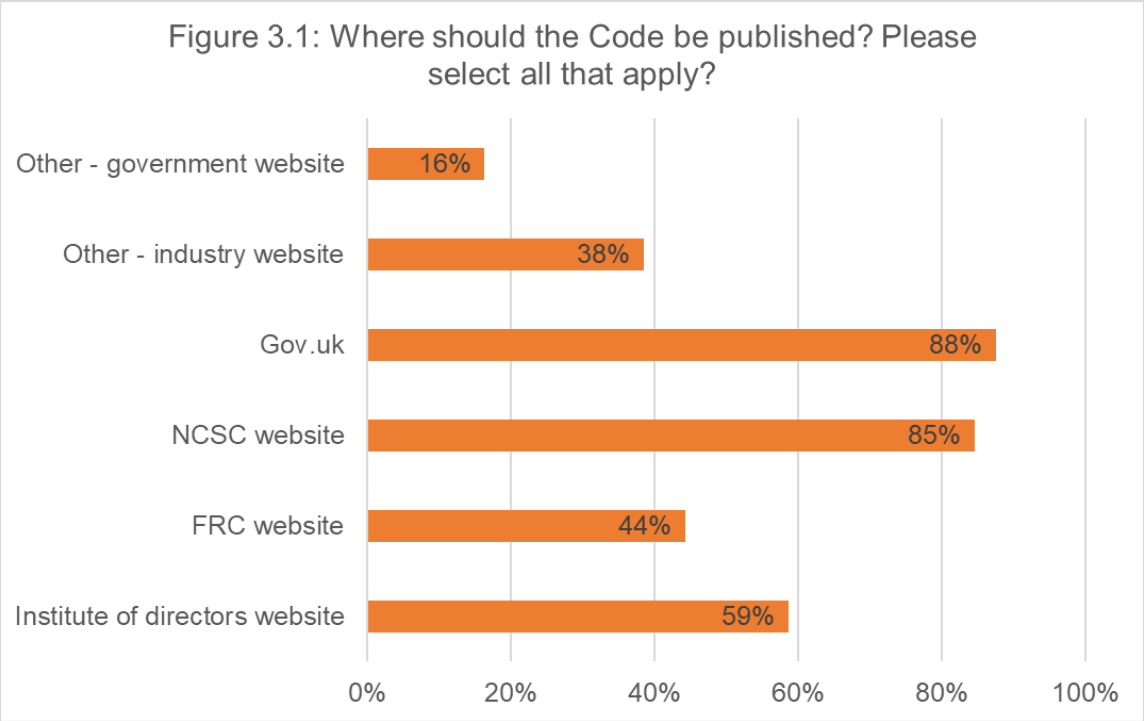
Base: 137

Q15: Are there any other actions missing from the current version of the Code of Practice



Base: 128

Q19: Where should the code be published? Please select all that apply.



Base: 104

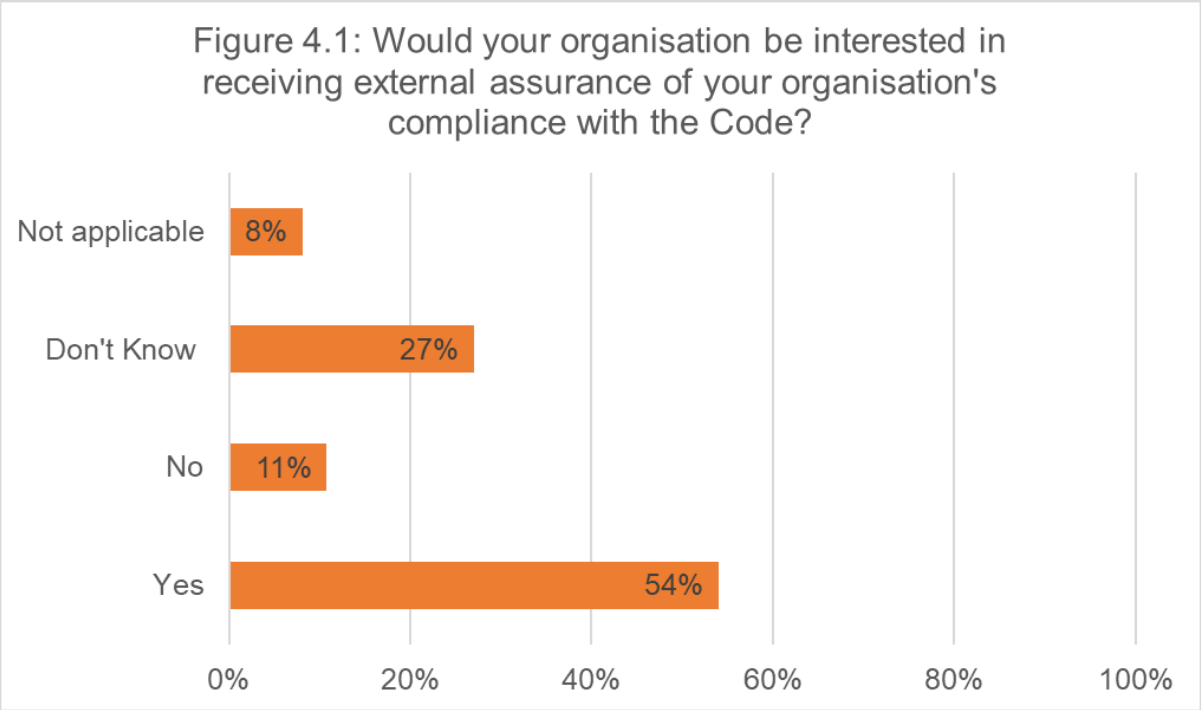
Q22: What organisations or professions could best assist in driving uptake of the Code with directors? Please select all that apply.

Table 1: What organisations or professions could best assist in driving uptake of the Code with directors? Please select all that apply.

Organisation/profession	Number	%
Asset management companies	27	27%
Auditors	64	63%
CISOs	72	71%
Company secretaries	45	45%
Insurers	60	59%
Investors	44	44%
Lawyers	35	35%
Regulators	68	67%
Risk/audit committees	76	75%
Shareholders	40	40%
Other	36	36%

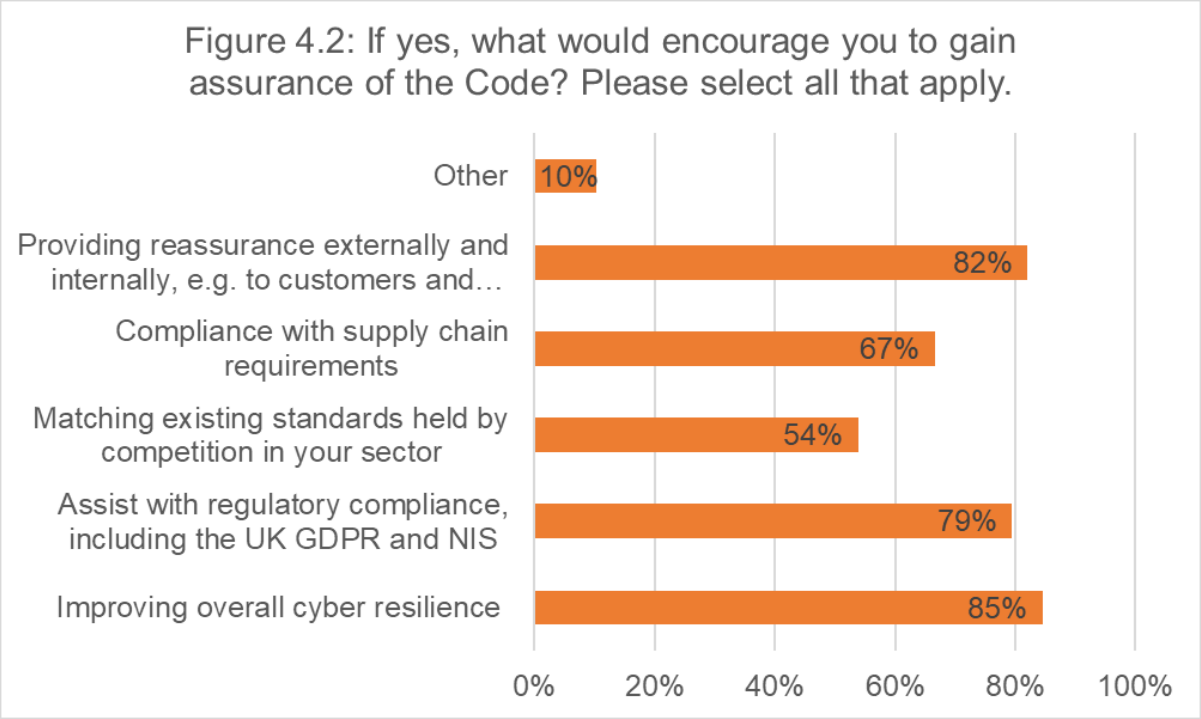
Base: 101

Q24: Would your organisation be interested in receiving external assurance of your organisation's compliance with the Code?



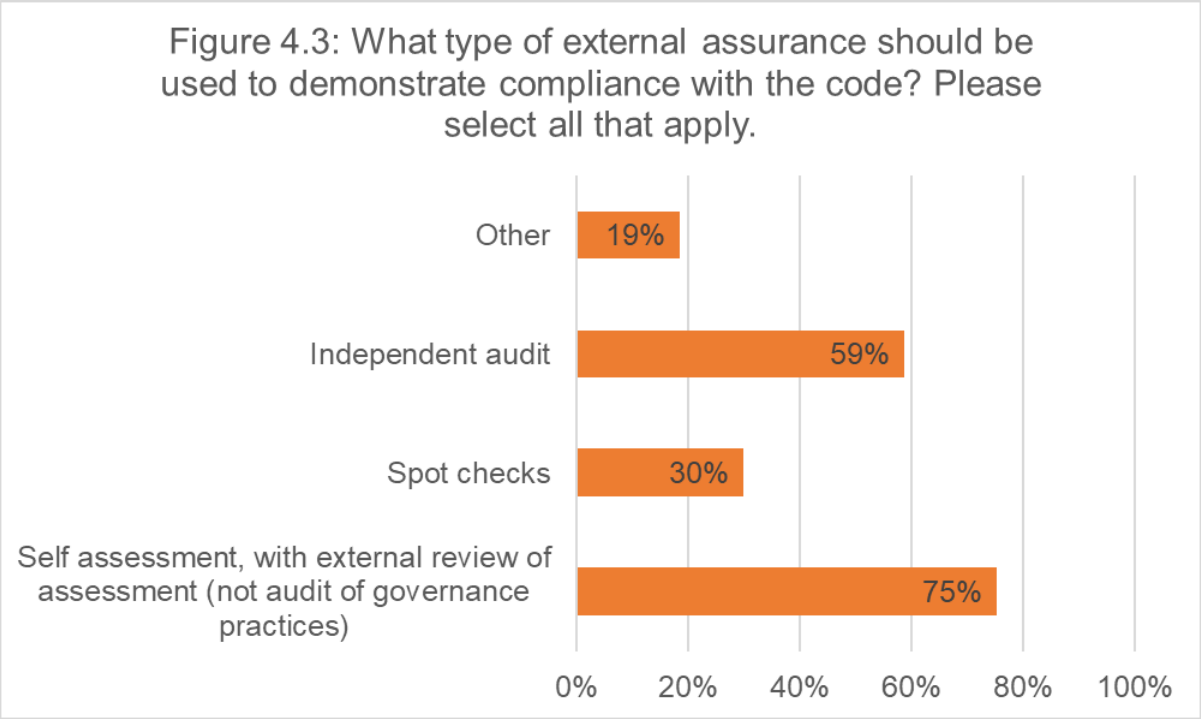
Base: 74

Q26: If yes, what would encourage you to gain assurance of the Code? Please select all that apply.



Base: 39

Q27: What type of external assurance should be used to demonstrate compliance with the Code? Please select all that apply.



Base: 97

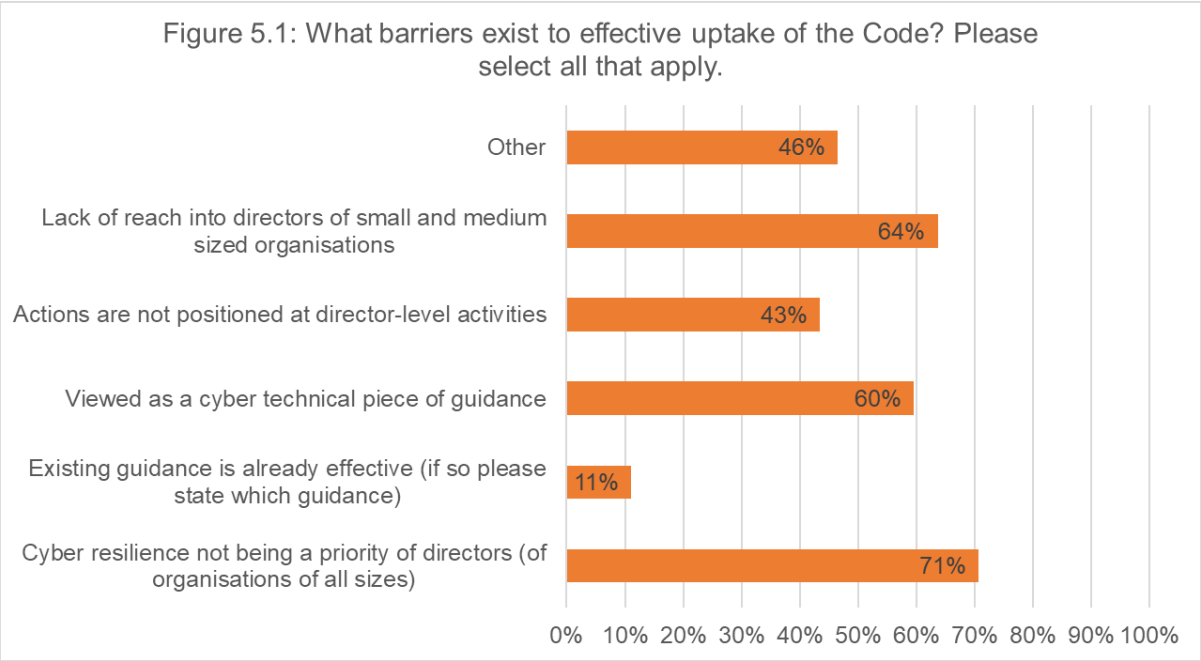
Q28: Which organisations or professions would place value on other organisations having received assurance against the Code? Please select all that apply.

Table 2: Which organisations or professions would place value on other organisations having received assurance against the Code? Please select all that apply.

Organisation/Profession	Number of responses	%
Asset management companies	37	41%
Auditors	57	63%
CISOs	57	63%
Company secretaries	33	37%
Insurers	67	74%
Investors	59	66%
Lawyers	33	37%
Regulators	70	78%
Risk/Audit Committees	63	70%
Shareholders	62	69%
None	3	3%
Other	25	28%

Base: 90

Q30 What barriers exist to effective uptake of the Code? Please select all that apply.



Base: 99

Annex B – survey questionnaire

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.
    - Under 10
    - 10–49
    - 50–249
    - 250–499
    - 500-999
    - 1,000 or more
    - 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:
    a. contact name
    b. organisation (if relevant)
    c. 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 (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
    - Compliance with GDPR
    - 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)

E03270244
978-1-5286-5412-8