techUK

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

DSIT Cyber Governance Code of Practice: call for views

Executive Summary

techUK and its members support the principles outlined in the Code of Practice for cyber governance, and the ambition to further strengthen resilience across the UK economy. However, members have expressed concerns around the potential for duplication of existing guidance which will create additional burdens for the sector, in particular small to medium-sized enterprises (SMEs) and risks market confusion rather than any value add.

techUK members would recommend the government documents its views on how enhancing the current standards could have a positive impact overall, giving more firmer detail as to what change the Code of Practice intends to drive. If pursued the Code should signpost to existing material which has been produced by standards bodies like ISO/IEC SC27 or explanatory content via stakeholders, such as the National Cyber Security Centre (NCSC). Alongside this, the Code should align with international norms and best practice should be clearly outlined to emphasise alignment with ethical and due diligence expectations.

To ensure good cyber governance, language should be used that resonates with executives and Boards to ensure there is investment from organisations and that the importance of good cyber governance is well understood.

Concerns about the skillset required for implementation was emphasised, along with the need for clear guidance, especially for SMEs facing capacity and funding limitations. techUK and its members recommend providing examples and creating checklists for Board members to drive uptake as added value content to existing international standards.

techUK and its members would also encourage the government to further collaborate with industry, and stakeholders, along with leveraging existing resources like the Cyber Essentials programme. The government should consider the types of incentives and levers that can be pulled in this space, that could support adoption and encourage good cyber governance.

Overall, techUK and its members stress the importance of evaluating existing practices, collaborating effectively, and providing clear guidance to ensure the successful uptake of cyber governance measures across sectors.

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]
    - Trade Association

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

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

Dan Patefield, Head of Programme, Cyber and National Security, techUK
Annie Collings, Programme Manager, Cyber and Central Government, techUK

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

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

- [✓ Yes]
- No
- Don't know

B: Cyber strategy

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

- [✓ Yes]
- No
- Don't know

C: People

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

- [✓ Yes]
- No

- Don't know

D: Incident planning and response

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

- [✓ Yes]
- No
- Don't know

E: Assurance and oversight

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

- [✓ Yes]
- No
- Don't know

12.Are there any principles missing from the current version of the Code of Practice?

- [✓ Yes]
- No
- Don't know

[If answered yes] Please set out any new principles that you think should be included and explain why. (1,800 characters)

techUK members broadly agree with the principles set out in the Code of Practice (the Code) but note concerns around reinventing standardised approaches which risk fragmenting the cyber skills base. Members also expressed concerns that the Code is not linked to any process to operationalise the new principles; and that small to medium-sized enterprises (SMEs) may face challenges due to their limited capacity and smaller budget allocations for such activities. Members, therefore, propose a review of existing publicly available guidance and standards to minimise duplication, reduce the additional burden on companies and better examine how SMEs can be supported to improve their operational response to cyber security in line with international standards.

techUK and its members propose to work with Government and wider stakeholders to enhance current standards and best practice. There are a number of proposed interventions both in the UK and internationally which touch on these issues. Where possible, approaches should be aligned and coordinated, given that the cyber security eco-system is truly global, with the majority of companies active in more than one nation/region.

In order to bolster support for cyber security governance, we would encourage the inclusion of best practice scenarios to illustrate the broader system benefits of such actions. This would serve as an incentive for Directors to take cyber security seriously and have a clear path to implementation. Additionally, our members suggest that a broader discussion should take place on how cyber governance fits within the existing ethical and due diligence expectations of a Board, including transparency and accountability.

Members have also highlighted the importance of stakeholders understanding the purpose of endpoint security. To ensure a business is secure from attacks the whole system needs to be protected, if there are vulnerabilities in systems even if through one device, this would be exposed during an attack. Members would like to see this clearly outlined and communicated to stakeholders. Members believe the risks from emerging technologies should be explicitly singled out with the government highlighting cyber security risks addressed in line with organisational approaches to the adoption of emerging technologies.

Drawing from government practices, particularly concerning supply chain security, members also suggest integrating relevant insights to strengthen the cyber security governance and emphasising the importance of addressing supply chain risk. One member noted that it would be worth engaging on this with the management committee of the Cyber Security Code of Practice Partnership (Energy Security), which is focused on supply chain risks. techUK acknowledges that government has also drafted a software vendors code of practice which is intended to address supply chain security, and so signposting to this in the Code would be beneficial. Indeed, as noted in the recent techUK response to the *'Protecting and enhancing the security and resilience of UK data infrastructure'* consultation, there is a complex set of current government activities which require clear communication to industry on how they interrelate.

techUK and members would also recommend that the Code does not diverge from established international norms. Established international best practices such ISO/IEC 27000 series or the existing national programmes like NIST Cybersecurity framework are already being used across the world. In the US, the Securities and Exchange Commission (SEC) set new rules in December 2023 to require public companies to disclose both material cyber security incidents and material information regarding their cyber security risk management, strategy and governance. For this reason, we would also recommend engaging with ongoing initiatives in US and Europe.

techUK would also note that any such Code must be subsidiary to recognised standards and sector specific codes and regulations. Organisations are covered by various obligations such as GDPR, NIS and more tailored sector specific regulations. Companies supplying the public sector are required to meet Cyber Essentials or Cyber Essentials plus, this on top of the government's plan on extending NIS and new codes for software vendors needs to be considered when publishing this Code.

Finally, members noted that the Code is missing a key issue around the skillset required to achieve its principles and actions in practice. Having some professional technical skill will be necessary to execute it, even if this is, for example, by employing a 'CISO as a Service' if the organisation is unable to afford a full-time CISO. We urge government not to proceed in such a way with a unilateral action that risks fragmenting the already scarce skillset, it is important people are trained and given guidance on behavioural expectations.

13.Are there any other actions missing from the current version of the Code of Practice?

- [✓ Yes]
- No
- Don't know

[If answered yes] Please set out any new actions that you think should be included and explain why. (1,800 characters)

techUK and its members broadly support the actions outlined in the Code of Practice, however, many of the actions are rather broad and subjective. We would, therefore, encourage the government to include additional information that directs organisations to publicly available standards and guidance, which aims to prevent overwhelming organisations. This is particularly pertinent for SMEs, who frequently face barriers due to capacity shortages and funding limitations.

Members have expressed concern about the multitude of risk assessments required for companies depending on its relevance and sector. Therefore, suggestions were made that government should outline the benefits of each risk assessment to assist companies in determining the most relevant assessment for their activity. Action 5 under 'Risk Management' should be enhanced to reflect the specific risks that should be assessed when reviewing suppliers, including the likelihood of supplier failure, service deterioration and concentration risk.

We would also recommend that SMEs could benefit from examples which illustrate the consequences of when organisations neglect to implement cyber governance. These examples would underscore the importance of the Code and highlight the repercussions of complacency.

techUK members advocate for the government to provide a checklist of questions for Board members to use when considering cyber security. This approach could promote more active participation and incentivise organisations to undertake the actions which are vital to their security. This includes having a clear view on the ongoing process for the management of key assets. It is important the government considers how it is incentivising businesses. There should also be clear identities within a business, to ensure the relevant personnel have access to the systems and data they need to do their job. For all organisations value for money is crucial, no more so than for SMEs. For this reason, guidance which supports them to raise their security maturity through straightforward measures is crucial, supporting them to get the basics right.

Management should assess and implement these responsibilities via commercially available and affordable solutions which are based on a standardised approach and have been independently reviewed. This would support the recognition of risks associated with emerging technologies as identified by the NCSC and other major national security agencies and follow risk identification and mitigation through people, processes and technologies in line with international standards.

While recognising the benefits of legislation as an incentive, members expressed concerns around its potential impact on SMEs. techUK would argue that the intent and ambition of this Code of Practice is made clearer upon publication. What improvements that might be seen would mean further government steps and interventions are not necessary, and vice-versa. Other Codes of Practice have seen elements incorporated in legislation, such as PSTI, and whilst there are certain benefits of that approach (enforced uptake, regulating at a clear baseline), it also brings risks (focus on compliance rather than best practice). techUK and its members are eager to work with Government to ensure that future steps and progress in this space are appropriate, necessary and practical for all parties.

14.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? (1,800 characters)

techUK and its members would stress the significance of referencing existing published standards and high-quality guidance within the Code of Practice, emphasising the need for clear signposting. Specifically, members highlighted guidance provided by the NCSC tailored to Boards, such as the Cyber Security Toolkit for Boards, as well as internationally recognised and accepted standards with full systems for voluntary accredited certification already in place.

Members have also underscored the value of tools like ‘Exercise in a Box’ offered by the NCSC. This online tool, which is freely available to businesses, enhances awareness of critical cyber incidents and generates resilience reports for organisations. Users of the tool can customise topics to suit their organisation’s needs at a basic level. It is recommended that Boards be directed to this tool as an example of improving cyber resilience and implementing best practices in cyber security. This is similar to the support given by the National Cyber Resilience Centre Group. These existing initiatives are all supported and utilised by industry and could be leveraged further here.

To see cyber governance adopted across sectors, a cultural change is needed. Without the proper incentives in place to adopt it this change will not be felt. Due to the significant investment that's already been given to programmes like Cyber Essentials and Cyber Essentials Plus, the government should consider how to sensibly incorporate cyber governance within these processes.

The Institute of Directors (IoD) offers professional development opportunities outlining best practices for Directors. techUK members also suggested leveraging insights from other government departments like the Department for Energy Security and Net Zero, which have already published relevant guidance as well as all the material covering the proper protection of personal data.

Finally, it is important to ensure that this information is publicly accessible; and we would caution against duplicating existing guidance. Furthermore, the government's messaging must be refined to help drive uptake and to support Directors to build cyber security into their organisation's structure. For example, risks should be mapped to business benefits and cyber should be articulated as a business enabler, rather than a technical inhibitor, in order to avoid a siloed approach.

15.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? (1,800 characters)

techUK and its members are in favour of the development of supportive tools to accompany the support for cyber governance. These materials should be developed in a language that resonates with the reader to ensure a clear understanding of their contents; and clear examples should be provided.

Members have suggested disseminating best practice information through existing standards, schemes and checklists published alongside recovery testing reports. This approach will reinforce business awareness of the most effective methods for creating cyber secure systems. Support for cyber governance should also direct organisations to existing areas of best practice. techUK members would also encourage the government to publish their research to help Directors to improve how they govern cyber security risk. This research will serve as a valuable tool for understanding the barriers organisations face when assessing their cyber maturity. It also benefits the broader cyber ecosystem by providing insights into challenges confronting business leaders. This research would also benefit industry engagement and the insurance sector more broadly.

techUK members would also recommend encouraging organisations to provide and share information on their cyber security risk management, strategy, and governance in an effort to promote and strengthen good practice across key sectors. This measure would support Chief Information Security Officers (CISOs), who often bear the responsibility of ensuring organisational security against cyber-attacks but may lack the necessary tools for effective implementation.

Several members have suggested establishing a formal approval process to define what constitutes good practice, enhancing transparency on the standards organisations are expected to meet as a baseline. Members propose utilising the expertise and international awareness of the British Standards Institute (BSI) to develop a Publicly Available Specification (PAS), promote and/or improve any perceived weakness in existing standards and utilise standardised accreditation and certification where third-party assessment is required.

Driving uptake questions

16.Where should the code be published?
Please select all that apply. [Multi-code]

- Institute of Directors
- FRC website
- NCSC website
- Gov.uk
- Other - industry website [free text to fill out]
- Other - government website: NCRCG

17.With whom should government (or the Code's owner if not government) work to promote the Code to ensure it reaches directors and those in roles with responsibility for organisational governance? (1,800 characters)

techUK members advocate for collaboration between the government and various stakeholders, including the IoD, NCSC, insurance companies, industry representatives, trade bodies such as the Federation of Small Businesses (FSB), and other government departments to ensure widespread awareness of the need for, and adoption of, good cyber governance. However, for this collaboration to be effective, the government must enhance its understanding of how to engage with Boards and their members. Members suggested using language which resonates with Directors to improve the uptake of the Code.

Members suggested exploring how to encourage organisations to appoint CISOs to Boards to ensure there is sufficient cyber security expertise and experience to implement good cyber governance.

The development of support for better cyber governance should involve input from all stakeholders to ensure its effectiveness. Furthermore, it is crucial that the approach be perceived as a business, rather than solely a cyber, action; and it should make clear to organisations the impact and implications of *not* implementing cyber governance. Companies must understand the level of risk they are exposed to, both for themselves and their customers, to take appropriate steps to enhance security against cyber threats.

techUK also encourages collaboration between the government and insurance companies to promote cyber governance. Some members flagged that as the insurance market drives behaviours it could help to enforce a voluntary standard: for example, companies demonstrating good cyber governance could potentially benefit from reduced insurance premiums, further incentivising adoption of best practice.

It is essential that stakeholders have public, cost-free access to the material that supports good cyber governance when published, ensuring widespread understanding and implementation. Further, organisations that could help government to disseminate such material include Local Enterprise Partnerships (LEPs), UKC3, the individual cyber clusters and the cyber resilience centres across the UK's nations and regions.

More broadly on building awareness, techUK members have highlighted that DSIT could look to the GDPR campaign work for a good example of how to drive uptake of cyber governance.

Finally, members highlighted the need to identify the right/optimum time to publish material to support cyber governance to ensure maximum visibility and successful uptake.

18.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? (1,800 characters)

techUK members recommend that government collaborates with companies providing Director training in the UK, working with them to integrate cyber governance into their training programmes. By making it clear that cyber governance is an essential part of a Director's role, it will naturally become ingrained in their responsibilities. Identifying any deficits in Directors' capabilities allows for targeted training, while increased awareness of the skills required to implement good cyber governance helps businesses identify where additional resources are needed to enhance network security.

techUK members would also emphasise the importance of the government understanding the motivations and behaviours of Directors at a Board level. They suggest using the COM-B behaviour model to deepen the government's understanding of the factors influencing Board decisions and the elements support for cyber governance must address to prompt Directors to take action or effect change within their organisations.

Members recommend drawing insights from the Association of Chairs, which supports Chairs and Vice Chairs in the charity and social enterprise sector in England and Wales. This organisation's hands-on approach provides valuable support, particularly for leaders and small business associations that may lack access to similar resources.

It is also suggested that the government leverage evidence collected through the UK Cyber Governance Project, highlighting the improved cyber resilience and reduced costs achieved by businesses implementing good cyber governance. This evidence can incentivise Directors to meet their Board's expectations regarding cyber security measures.

To bolster the uptake of Board level good cyber governance, members propose creating a model for implementation targeting SMEs. This approach enables organisations to replicate the implementation model effectively.

19.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]
    - General IT support staff in SMEs

[If answered 'Other'] Please set out any other market stakeholders not included and explain why. (1,800 characters)

The government should also work with the banking sector and cyber vendors who can support to increase the uptake of guidance on cyber governance. Indeed, as a tool to sign post existing resources and case studies, industry (including Managed Service Providers who will come under the scope of the NIS Regulations when updated) will help drive uptake of good cyber governance by sharing it with clients and prospective clients.

Assurance questions

20.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

Please explain your answer. (1,800 characters)

techUK members have raised several concerns regarding the potential impact of external assurance on organisations. It is essential to clarify the purpose of external assurance to understand its benefits for organisations. While larger organisations may view external assurance as a measure of maturity and professionalism, smaller organisations may find it competitive and fear it exacerbates the gap between large and small entities. Making external assurance a requirement of the Code would complicate matters for organisations as well as drive up costs through the creation of a 'cottage industry' to carry out the assurance. It would fragment the skills base and become a non-tariff trade barrier if adopted as a public sector requirement.

Organisations already have the option of certification against ISO standards and Cyber Essentials requirements to adhere to (noting the latter is already a requirement for UK public sector markets), and therefore some members highlighted that they were not in favour of further assurance but would rather focus on identifying practical activities that will drive cyber resilience.

Overall, techUK and its members would urge the government to evaluate existing external assurance requirements for businesses to avoid duplicating material already available. This approach aims to alleviate additional burdens on businesses and potentially improve the uptake of cyber governance by not imposing additional obligations nor fragmenting the skill base and supporting internationally recognised approaches. For example, government could consider linking its work on cyber governance to existing external assurances already in the public domain, such as those provided by the Prudential Regulation Authority (PRA). Some members suggested expanding Cyber Essentials to incorporate governance, which could potentially offer a route to building greater resilience.

21.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]

22.What type of external assurance for demonstrating compliance with the code would be of greatest interest?

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]

23.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]

[If answered 'Other'] Please set out any other market stakeholders not included and explain why. (1,800 characters)

techUK members would also encourage the government to engage with industry bodies across all sectors to this end, as the cyber security eco-system is vital to all organisations across the UK economy.