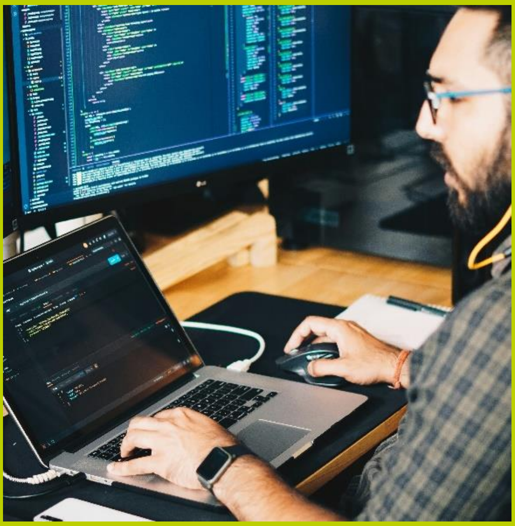
Cyber Governance Code of Practice Call for views:

BCS response



Executive Summary

This is the response from BCS, The Chartered Institute for IT to the government’s call for views on its draft Cyber Governance Code of Practice to help businesses and organisations manage the cyber risks they face.

The Code sets out the critical governance areas that directors need to tackle in order to protect their organisations. The Code is designed to be simple to use, with the relevant information all in one place. It is for organisations of all sizes.

A panel of BCS Information Security Specialist Group (ISSG) experts welcomed the DSIT proposal to engage directors on information and cybersecurity governance. Our panel agreed with the previous findings of the government's Cyber Security Incentives and Regulation Review Call for Evidence 2020 that many directors 'find the cyber landscape complex and challenging to navigate’. That consultation found that 83% of those surveyed stated that there is a need for additional solutions to illustrate 'what good looks like'. One solution could be a greater emphasis on objective criteria to define good practice in the suggested actions of the Code of Practice.

The Cyber Governance Code of Practice set out five overarching principles; (i) risk management; (ii) cyber strategy; (iii) people; (iv) incident planning and response; and (v) assurance and oversight. All were all welcomed by the ISSG panel.

However, the panel felt a mandatory Code of Practice with annual reporting might be more effective than a voluntary code, with board members held accountable for their company's cyber security throughout its lifecycle.

The panel agreed with the proposed approach outlined in the consultation to develop a Code of Practice that would be 'simple to engage with, for organisations of all sizes.' This would be helpful for SMEs in particular because, unlike larger enterprises, smaller firms don't necessarily have access to or employ cyber experts at the board level.

Design questions

This section called for our views the five principles in the Code of Practice that were co-designed with NCSC and industry experts. It asked 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

B: Cyber strategy

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

· Yes

C: People

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

· Yes

D: Incident planning and response

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

· Yes

E: Assurance and oversight

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

· Yes

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

· Yes

As we answered yes – we were asked to set out any new principles we thoughts should be included and explain why.

While agreeing with the five main principles overall, the ISSG panel is concerned that this is a voluntary Code of Practice. The panel knows from their experience working in this sector that cyber risk is often low on the agenda of many boards; hence, a mandatory Code of Practice would be more likely to focus the attention of board members and directors on this critical issue.

The panel would also like the Code of Practice to be more explicit regarding the accountability of directors/ board members, including non-technical ones.

Following the deployment of a cyber security strategy, the board must also be able to address and be accountable for any issues that might arise in an ethical, competent manner, applying the highest professional standards.

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

· Yes

While welcoming the idea in Action E of 'formal reporting on at least a quarterly basis,' the panel also suggests it would be better if this guidance went further. The panel advises legislation requiring organisations to report on cyber risk management and incidents annually, similar to those submitted for financial accounts, health and safety and ESG.

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?

While agreeing it's essential to keep the Code of Practice understandable for all, the actions suggested in Annex A should be linked to established information, cybersecurity frameworks, and standards. This would enable organisations to 'map' their current arrangements to well-defined, well-understood and well-established frameworks.

Many larger organisations wanting to improve their cyber governance would wish to align themselves to such frameworks or standards (e.g. NIST 2.0, ISO27001, and Cybok).

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?

Organisations may find it easier to understand 'what good looks like' if more of the suggested actions in Appendix A include some objective criteria.

The current cyber essentials programme, owned by NCSC, requires certifying organisations to assess against five technical areas. The NCSC should consider extending this programme to include cyber governance.

The panel also reiterated its advice from a previous consultation, Cyber resilience of the UK's critical national infrastructure, that the government should create a 'one-stop shop' for advice on cyber security (which may be the NCSC) in a similar way to the ICO, which caters for organisations in differing sectors and of different sizes.

Driving uptake questions

16. Where should the Code be published?

Please select all that apply. [Multi-code]

· Institute of Directors ✓

· Federation of Small Businesses ✓

· FRC website ✓

· NCSC website ✓

· Other: industry website IASME ✓

· Other: ISSG suggest a one-stop shop for cyber security for all organisations on the government website - gov.uk ✓

· Other: UKAS ✓

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

As pointed out in the background accompanying this consultation, several organisations already provide cybersecurity advice, which can create information overload for directors. Our panel felt the government (or the Code's owners) needed to consolidate information and position it in relation to existing guidance to avoid confusion.

It would also benefit the government to work with organisations that represent small and medium companies to understand their needs better. The panel said SMEs could need help assigning specific responsibilities for cyber at a board level or to employ a CISO. Our panel advised that the language and terminology in the Code of Practice should be explicitly "low context" rather than "high context" language, which requires significant prior tacit domain knowledge.

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?

The current cyber essentials programme, owned by NCSC, requires certifying organisations to assess against five technical areas. It would be advisable for the NCSC to consider an extension of this programme to include aspects of cyber governance should be considered.

The Code of Practice should also be incorporated into the existing guidance, standards, regulations, and frameworks considered while developing this draft Code of Practice.

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 ✓

Assurance questions

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

- Not applicable

21. If yes, what would encourage you to gain assurance of the Code?

- Not applicable

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

Please select all that apply.

- Self-assessment, with external review of assessment (not audit of governance practices) ✓
- Spot checks ✓
- Independent audit ✓

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

- Asset Management Companies ✓
- Auditors ✓
- CISOs ✓
- Company Secretaries ✓
- Insurers ✓
- Investors ✓
- Lawyers ✓
- Regulators ✓
- Risk / Audit Committees ✓
- Shareholders ✓

Barriers to implementation

24. What barriers may exist to effective uptake of the Code?

Please select all that apply

· 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 small and medium-sized organisations' directors ✓

Conclusion

25. Additional Feedback from ISSG.

There is the possibility that unless this latest Code of Practice on Cyber Security governance is clearly labelled as the overarching guidance, then it could potentially confuse or dilute advice from other sources already available.

It was also noted that the document focuses on people, which can be helpful in engaging directors, especially those who are non-technical. However, there is also a need for more details about processes and technology for those firms who can process this information.

ISSG Panel

A subgroup of the BCS ISSG responded to the call for views:

- Steve Sands CITP FBCS MCIIS, chair of the ISSG and a risk and compliance professional with a background in information security, IT management and data protection.
- Ms Wendy Goucher MSc (Res) FBCS Information Security and Risk Consultant, vice chair of ISSG. Wendy works with organisations to devise policy and procedures that are compliant with external rules and operationally effective.
- Patrick Burgess CITP MBCS cofounded Nutbourne, a Managed Service Provider, and is also the Founder of Clearbenchmark, a SaaS company helping MSPs reduce their clients' exposure to risks. He is a CompTIA MSP Industry Instructor and won their 2023 Cyber Security Leadership Award.
- Angus Pinkerton CISSP, MBCS, FIES, is a consultant in information security strategy based in Scotland with a background in the nuclear industry.
- Tim Williams CITP FBCS MCIIS is a senior security, business and IT consultant in government and financial services.
- Andrew Wright CISSP CISM CITP MBCS PMP is a Senior NHS Digital Leader specialising in Cyber and Information Security in NW London

bcs
The
Chartered
Institute
for IT