IET Response to DSIT Cyber Governance Code of Practice

The responses to the survey questions below should be read in conjunction with the DSIT Cyber Governance Code of Practice Proposal and Call for Views.

IET responses are highlighted in yellow.

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: Professional Engineering Institution

3.[if organisation] How many people work for your organisation across the UK as a whole?

- 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. Andrew Rylah, policy@theiet.org, Institution of Engineering and Technology

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.
- Consideration of emerging technologies and innovation in cyber security could be explicitly included to ensure organisations are prepared for future challenges.
- Recognition of professionalism for cyber security practitioners, including existing schemes backed by Government and professional membership organisations. The IET is the leading Professional Engineering Institution in the UK and supports engineers and technicians in gaining professional registration through the Engineering and UK Cyber Security Councils.

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.
- Guidance on engaging with third-party vendors and partners to ensure end-to-end cyber resilience in the supply chain could enhance the Code's comprehensiveness.

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?

- References to ISO 27001, NIST's Cybersecurity Framework, and the NCSC's Cyber Assessment Framework can provide directors with a solid foundation for understanding and implementing best practices in cyber governance.
- Reference to professional recognition for cyber security practitioners through registration with Engineering Council, UK Cyber Security Council and the BCS. The IET supports engineers and technicians in gaining such professional registration.

The adoption of cyber governance is important for all businesses. That said, the guidance must be proportionate, applicable, scalable, and understandable by non-specialists. This is so it can be applied equally to smaller and larger organisations, with appropriate granularity and taking account of the sensitivity and connectedness of the environment in which the business operates.

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?

- Checklists for regular cyber health checks, templates for incident response planning, and indicators of good practice ('green flags') for effective cyber governance should be included, to aid practical implementation. These tools should be designed to be practical, enabling directors to navigate the Code's requirements more efficiently and strengthen their organisation's cyber resilience. Examples include:
  - Step-by-Step Checklists: For conducting cyber health checks and ensuring compliance with each principle of the Code.
  - Incident Response Templates: Customizable templates for developing and executing incident response plans.
  - 'Green Flags' Indicators: Quick-reference indicators of good practice for effective cyber governance, helping directors identify and aim for best practices in cyber resilience.
  - Cyber Resilience Scorecard: A tool for organisations to self-assess against the Code's framework, highlighting strengths and areas for improvement.
  - Guidance on Cyber Security Tools: Advice on selecting and optimizing cyber security tools to avoid overload and focus on tools that offer the most value, based on the organisation's risk profile.
  - Supplier Risk Assessment Criteria: A framework to consistently evaluate and manage the cyber security risks associated with suppliers and partners.

Driving uptake questions

19.Where should the code be published?

Please select all that apply.

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

The Institution of Engineering and Technology

The UK-Cyber Security Council and Companies House websites at a minimum. It should also include Industry bodies, for instance CBI, Federation of Small Businesses plus trade bodies. This is to ensure it reaches a wide audience across different sectors.

20.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)

Collaboration with industry bodies (trade bodies, Chambers of Commerce, the CBI, FSB etc), professional bodies (including Professional Engineering Institutions) and sector-specific regulators can help promote the Code effectively to its target audience. The IET would be happy to support the government's objectives in this regard.

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? (1,800 characters)?

Director training programmes, accreditation products and existing guidance frameworks can incorporate the Code to enhance its uptake and practical application.

The guidelines should be included in Director training and professionalism courses and organisations, such as the Institute of Directors' "Chartered Director". There would also be benefit from including details in the Engineering Council's, BCS and UK Cyber Security Council's chartered engineering / IT / security professional qualifications.

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]
- [If answered 'Other'] Please set out any other market stakeholders not included and explain why.

23. Local authorities, suppliers to Critical National Infrastructure (CNI), public bodies, (emergency services, etc.) should mandate these recommendations to their suppliers, given the potentially significant consequences and the need for major incident planning / business continuity. Regional cyber resilience centres, regional cyber clusters, and their national equivalents should be consulted to help drive engagement and uptake.

Assurance questions

24.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.

26.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 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]

An independent audit would provide the most credible form of assurance for demonstrating compliance with the Code.

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
- [If answered 'Other'] Please set out any other market stakeholders not included and explain why. Trustees

29. The highlighted parties would greatly value assurance against the Code for transparency and confidence in cyber governance practices.

Barriers to implementation

30.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
- Other [please specify]

The perceived complexity of implementing the guidance could also be a significant barrier.

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
- [If yes], Please set out your additional feedback in the box below. (500 words)

Dealing with key issues:

- Low uptake of cyber security assessments: Propose mechanisms to incentivize/mandate assessments across the broadest spectrum of organisations
- Limited Understanding of Supply Chain Security: Strengthen the recommendations on organisational assurance/risk assessment, providing detailed guidance on understanding/securing supply chains effectively.
- Low Penetration of Cyber Essentials: Recommend integrating recognized frameworks/certifications into its practices. Emphasize the importance of broader participation.
- Flaws in Self-Attestation Mechanisms: Advocate robust, independent verification methods beyond self-attestation to ensure reliable cyber-risk assessments.
- Tool Overload & Analysis Paralysis: Simplifying cyber-risk management tools and processes, emphasizing the importance of actionable intelligence/prioritization in decision-making to prevent overwhelm/inaction.
- Challenges in Assessing Supplier Risks: Add concrete, scalable approaches/frameworks that organisations can use to assess numerous suppliers without exhausting resources.

Recommendations

- Assessment incentives: Introduce incentives for conducting and regularly updating cyber security assessments, eg through tax breaks / reduced insurance premiums.
- Guidance on Supply Chain Security: Offer steps for assessing/securing supply chains, eg. through industry groups partnerships to develop sector-specific guidelines.
- Cyber Certification Participation: Encourage certifications through government subsidies, awareness campaigns, or linking certification to contract eligibility.
- Promote professional recognition eg. through the UK Cyber Security Council / Engineering Council / BCS
- Assurance Mechanisms: Advocate a mix of self-assessment/independent audits for critical sectors. Establish a registry of accredited/assessors for quality and reliability.
- Tool Usage: Recommend best practices for consolidating/optimizing cyber security tools. Provide guidance on interpreting/prioritizing the findings for effective action.
- Scalable Supplier Risk Assessment: Develop and share tools, methodologies, or platforms for scalable/efficient assessment of supplier risks.

Cyber security governance must be treated as a continuous process, not a one-time compliance exercise.

The guidance can significantly improve/extend cyber resilience effectiveness across organisations of all sizes/sectors. The IET would welcome the opportunity to further the Code's reach and impact.