



Department for
Science, Innovation
& Technology

Feryal Clark MP
Parliamentary Under Secretary of State
(Minister for AI and Digital Government)
22-26 Whitehall
London SW1A 2EG

Chi Onwurah MP
Chair, Science, Innovation and Technology Committee,
House of Commons,
London,
SW1A 0AA

08 April 2025

PUBLICATION OF THE CYBER GOVERNANCE CODE OF PRACTICE

Dear Chair,

I am writing to notify you of the launch of the Cyber Governance Code of Practice, which my department has published today. We wrote to your committee in January 2024 to inform you of the launch of our call for views, and in January 2025 to inform you of the publication of the government response to a call for views. Please see enclosed a copy of the Cyber Governance Code of Practice.

Background

The effective governance of cyber security risk by boards and directors is integral to each organisations' resilience and competitiveness, and the collective resilience of the UK's economy. As the use of emerging technologies such as Artificial Intelligence (AI) continue to grow, so does the cyber risk that is associated with the increasing reliance on technology.

Building and maintaining cyber resilience is therefore crucial to protecting the safety of individuals and the growth of the UK economy. By governing cyber risk effectively, organisations can better safeguard customers personal data and take full advantage of digital technologies which can drive the business strategy and deliver efficiencies.

However, despite government and industry action over the course of subsequent national cyber strategies, including the world-class guidance and support developed by the National Cyber Security Centre (NCSC), research shows that many businesses of all sizes are still failing to adequately protect themselves against cyber attacks. One of the contributing factors is a lack of understanding and ownership at the most senior levels.

The Cyber Governance Code of Practice

Given that cyber risk is a principal risk for almost all organisations, boards and directors need to be able to govern this risk effectively. To help support them, DSIT has launched the Cyber Governance Code of Practice (the Code). The Code will support boards and directors in knowing what actions they should take, or ensure are taken, to enhance the resilience of their organisation.

The Code forms part of a package of action on cyber governance which DSIT and NCSC has worked with industry to create. The Code should be used as the first point of reference for board members as it sets out the most critical governance actions that directors need to take ownership of. It is underpinned by Cyber Governance Training, which helps boards and directors to strengthen their understanding of how to govern cyber security risks; and the Cyber Governance Board Toolkit, which supports board and directors in implementing the actions set out in the Code.

This work on cyber governance is also aligned with DSIT's other cyber security initiatives, such as the Cyber Security for AI Code of Practice and the upcoming Software Vendors Code of Practice, which will both improve security practices, outcomes, and confidence for UK organisations.

Next Steps

During the call for views which ran from January-March 2024, industry asked that government engage with a wide range of stakeholders to encourage uptake of the Code. Following this feedback, DSIT will work with industry to drive uptake of the Cyber Governance Code of Practice and the wider cyber governance package through a voluntary public pledge.

Yours sincerely,

A handwritten signature in dark ink, appearing to read 'Feryal Clark', is positioned above the printed name.

Feryal Clark MP
Parliamentary Under Secretary of State for AI and Digital Government