PETER BASSILL · PETERBASSILL.COM/NED

The Cyber and AI NED Charter

A public, citable definition of the Cyber and AI Non-Executive Director discipline. Use this to frame a brief, structure a candidate search, or evaluate an existing appointment.

What this is

A Cyber and AI Non-Executive Director is a board-level independent director with practitioner-grade expertise in both cyber security and artificial intelligence governance, in a single seat. The combination matters because the regulatory regimes are converging, the failure modes interleave, and the alternative — two specialists who cannot answer each other's questions — is structurally more expensive and structurally less effective.

Why this is one discipline, not two

AI systems are cyber-security targets — training data is a poisoning surface, model weights are a theft target, inference endpoints are subject to prompt injection and resource exhaustion. **Security tooling is increasingly AI-driven** — modern SOCs run on classifiers, clustering, agents, and LLM-based triage. **Regulators have already converged** — the EU AI Act cross-references NIS2; DORA cross-references both; the UK Cyber Governance Code is being designed to interoperate with the work emerging from the AI Safety Institute. A NED who is fluent in only half of this surface is governing only half of the picture.

Regulatory regimes covered

- **Companies Act 2006** — directors duties, sections 171–177, including the higher s.174 standard for specialist NEDs.
- **UK Corporate Governance Code (FRC, 2024 edition)** — principal-risks framework and the strengthened risk-and-control declarations from 2026.
- **UK Cyber Governance Code of Practice (NCSC / DSIT)** — board-level cyber-resilience expectations.
- **FCA SYSC 15A** — operational resilience for in-scope financial services firms.
- **NIS2 Directive (Article 20)** — management body liability for cyber-risk oversight; broader scope than NIS1.
- **Digital Operational Resilience Act (DORA, Article 5)** — ICT risk-management framework; financial-services and their ICT third parties.
- **EU AI Act (Regulation 2024/1689)** — high-risk AI obligations, AI literacy, conformity assessments, and sanctions up to €35m or 7% of global turnover.
- **UK GDPR / Data Protection Act 2018** — DPIAs, automated-decision provisions, ICO enforcement.

When boards most need this seat

- **Post-incident** — the technical issues are fixed but the governance gap remains.
- **Pre-fundraise or pre-IPO** — investor diligence is flagging cyber and AI governance as material.
- **Newly-regulated** — NIS2, DORA, or the EU AI Act high-risk provisions bring the company into scope.
- **AI-deploying** — production AI is going live in a regulated decision-making context.
- **CISO transition** — the CISO is leaving, has left, or is signalling they will.
- **Acquirer-side** — diligence on the cyber and AI posture of an acquisition target.

The role in practice

Reads the board pack with a domain-literate eye. Sits on the Audit, Risk, or Technology Committee. Holds standing one-to-ones with the CISO and the head of AI between meetings. Is on the phone within hours of a serious incident. Reviews the AI register, the DPIAs, and the third-party / supply-chain risk profile. Brings regulator-readiness as standing posture, not crisis response. Personally liable as a statutory director under the same duties as the executive directors.

Read the full essay at **peterbassill.com/ned/cyber-and-ai**. Engagement process and fee ranges at **peterbassill.com/ned/engage** and **peterbassill.com/ned/cost**. First call is free, exploratory, and explicitly scoped as 'I will tell you if I think you do not need me yet'.