

# EXECUTIVE SUMMARY FOR THE BOARD CHAIR

## The 4-Hour Clock: Board Liability Under DORA, NIS2, and AI Regulation

Pre-Authorised Command Architecture | Personal Liability Protection | 90-Day Blueprint

<b>4 Hours</b> DORA Initial Report	<b>5 Clocks</b> Simultaneous Regulatory	<b>€1M</b> Personal Director Fine	<b>€345M+</b> Combined Exposure (illustrative €2B entity)	<b>90 Days</b> Implementation Blueprint
---------------------------------------	--	--------------------------------------	--	--

### WHY THIS MATTERS TO YOU PERSONALLY

DORA Article 5 (effective 17 January 2025) and NIS2 Article 20 (transposed across EU) establish personal accountability for cybersecurity governance at the management body level. This accountability is personal and cannot be delegated. Personal fines reach €1M under DORA. NIS2 empowers regulators to impose temporary bans from management positions. Delegation to the CISO or IT team does not shield directors from personal responsibility. 67% of boards acknowledge their practices are inadequate (WEF Global Cybersecurity Outlook 2025). Only 2% of organisations have firm-wide cyber resilience.

### THE FIVE REGULATORY CLOCKS YOUR NEXT MAJOR INCIDENT WILL TRIGGER

Regulation	First Report	Your Personal Risk
DORA	4 hours	€1M personal fine; suitability review
NIS2	24 hours	Management ban; €10M entity fine
EU AI Act	2-15 days	Up to 7% global turnover
SEC	4 business days	Personal enforcement (e.g., SolarWinds CISO)
UK CSR Bill	24 hours	£100K/day continuing penalty

### THREE BOARD RESOLUTIONS REQUIRED WITHIN 30 DAYS

- **Resolution 1 — Command Architecture:** Approve Gold/Silver/Bronze command tiers with named decision authorities for all five regulatory clocks. Pre-authorise SILVER tier to handle initial regulatory notifications without board escalation.
- **Resolution 2 — Risk Framework:** Approve the ICT Risk Management Framework including incident classification thresholds aligned to DORA/NIS2 definitions, pre-built notification templates, and a documented mandatory training programme.
- **Resolution 3 — Third-Party Oversight:** Formally approve the Register of Information for all ICT third-party providers (DORA Art. 28(3)) and mandate quarterly board reporting on resilience metrics.

*(Draft board resolutions for each item above are included in the accompanying board pack.)*

### CLOSING THE D&O; INSURANCE GAP

A critical blind spot for many boards: 38% of directors face a D&O; coverage gap for cyber-triggered personal liability (WTW 2024). The Insurance Safe Harbor Evidence Checklist (see Section 12.2 of the full whitepaper, included in the accompanying board pack) provides eight documented evidence items that demonstrate active governance. Boards presenting this portfolio to D&O; insurers may secure premium reductions exceeding 20% (Risk Strategies 2025). Organisations with formalised board oversight outperform peers by 5% in total shareholder return over three years (MIT CISR 2025).

### 90-DAY IMPLEMENTATION TIMELINE

Phase	Timeline	Your Role	Est. Cost
Command Design	Days 1-21	Approve charter	£75-120K
Regulatory Mapping	Days 22-45	Review gap report	£150-250K
Controls Deployment	Days 46-75	Dashboard review	£200-400K
Board Integration	Days 76-90	Sign resolution + training	£100-180K

**Total programme cost: £525K–£950K** (typically <0.5% of annual IT budget) vs. combined regulatory exposure of €345M+ (illustrative €2B entity). Implied governance return multiple: c.350:1.

**IMMEDIATE ACTION FOR THE CHAIR:** Mandate a 60-minute board briefing at the next meeting on DORA/NIS2 personal liability, to precede approval of the three resolutions at the following board meeting. The full whitepaper, implementation toolkit, and tabletop exercise scenarios are available for formal agenda inclusion.

*This 1-page summary is accompanied by a full board pack and tabletop scenarios for formal agenda inclusion.*

Kieran Upadrasta | CISSP, CISM, CRISC, CCSP | MBA | BEng | 27 Years Big 4 Consulting (Deloitte, PwC, EY, KPMG) | Schiphol University  
[info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) | [www.kie.ie](http://www.kie.ie) | [linkedin.com/in/kieranupadrasta](https://www.linkedin.com/in/kieranupadrasta)

© 2026 Kieran Upadrasta / Cyber AI Systems Inc. All rights reserved.