Workshop 5 – Digital Governance, AI, Cybersecurity and DORA Oversight

Date: 16th July

Time: 09:00 – 14:00

Workshop Facilitator: Prof. Maria Lucia Passador, formerly Assistant Professor of Corporate Law and Financial Markets Regulation

The session will focus on **Digital Governance, Artificial Intelligence, Cybersecurity and DORA**, with particular emphasis on the fiduciary responsibilities of boards of directors and senior executives. The central idea is that digital transformation, AI adoption and cyber resilience are no longer merely technical or operational matters: they have become core governance issues, directly affecting directors' duties, risk oversight, organisational accountability and strategic decision-making. More specifically, the session will be structured around three main areas:

Agenda

Time	**Session**
09:00 – 10:30	**Session 1 – Digital Governance & AI**
This part will explore how boards and senior management should approach AI and digital technologies from a governance perspective. It will consider how AI-related risks — including explainability, bias, accountability, third-party dependency and regulatory compliance — should be translated into internal controls, reporting lines and board-level oversight. The discussion will also touch on practical use cases, including AI in credit scoring, HR recruitment, board reporting and cyber incident management.	
10:30 – 11:00	**Coffee Break**
11:00 – 12:00	**Session 2 – Cybersecurity & DORA Oversight**
The second part will focus on cybersecurity and digital operational resilience, with particular reference to DORA. The session will address how DORA should be understood not only as a compliance framework, but also as a governance framework requiring active board supervision. Particular attention will be given to ICT risk management, incident response, third-party providers, concentration risk, internal controls, audit evidence and the documentation of oversight.	

12:00 – 12:45	**Lunch Break**
12:45 – 14:00	**Interactive Group Case Study**
The final part will examine digital trust as a strategic asset. It will consider how boards can move beyond a defensive compliance approach and instead treat digital resilience, AI ethics and cyber preparedness as elements of long-term corporate value. This will include discussion of ESG and stakeholder expectations, digital trust in M&A and procurement, internal culture and AI literacy, and the need for directors to be able to challenge, approve, supervise and document decisions involving digital technologies. Overall, the session is intended to provide participants with a board-level framework for understanding digital, AI and cyber risks, and for integrating them into corporate governance, fiduciary duties and strategic oversight. The key takeaway is that boards do not need to become technologists, but they must be able to ask the right questions, understand the risk architecture, ensure appropriate escalation and accountability, and document meaningful oversight.	**Strategic Digital Trust & Board Leadership**
14:00 – 14:15	**Wrap-Up, Key Takeaways & Close**