FLORENCE SCHOOL OF BANKING AND FINANCE

EXECUTIVE TRAINING COURSE

PROGRAMME

Managing financial sector cyber risk

4 May - 26 June 2026

Ten years of excellence,
shaping knowledge for tomorrow

2016 - 2026

www.fbf.eu

Co-funded by
the European Union

Introduction

This course, organised in collaboration with IOB, introduces cybersecurity in the banking and finance sector, focusing on risks arising from digital transformation and highly interconnected systems. It covers core cyber threats, regulatory frameworks, resilience strategies, and the geopolitical and technological forces shaping cyber risks in banking and financial services. Participants will develop practical and strategic skills to assess vulnerabilities, manage incidents, and strengthen resilience in an increasingly AI-driven financial landscape.

Course Directors

- Diarmuid Murphy | IOB
- Daria Vernon De Mars | EUI-FBF

Format | Online

Level | Introductory

Approach | Qualitative

Learning Objectives

- Understand cybersecurity risks and vulnerabilities specific to the digital finance ecosystem.
- Identify key threat actors and attack vectors targeting financial institutions.
- Apply core principles of cyber resilience, including ICT risk management and threat intelligence.
- Navigate international standards and EU cybersecurity regulations relevant to the financial sector.
- Assess the strategic impact of geopolitics and AI on the evolving cybersecurity landscape

Target audience

The course is designed for professionals working in public institutions and the private sector.

OUTLINE OF THE COURSE

Module 1: Digital finance and the cyber threat landscape

1.1 Live Class 1: Digital finance and cyber risk (60 mins | 7 May)
1.2 Anatomy of attacks: from phishing to advanced persistent threats
1.3 Threat actors' ecosystem: from hackers to State-backed operations

Module 2: Foundations of cyber resilience

2.1 Live Class 2: Principles of ICT risk management (60 mins | 14 May)
2.2 Cybersecurity deep-dive: understanding cyber threat intelligence
2.3 Cyber crisis communication and managing reputational risk

Module 3: Governance, global standards and regulatory frameworks

3.1 Live Class 3: Global standards and cyber governance basics (90 mins | 19 May)
3.2 Live Class 4: The EU regulatory landscape (90 mins | 21 May)
3.3 Lessons in cyber governance from financial authorities

Module 4: The geopolitics and geoeconomics of cyberspace

4.1 Live Class 5: The cyber-geopolitical order: systemic risks, sovereignty, and financial stability (90 mins | 26 May)
4.2 Live Class 6: The new digital battlefield (90 mins | 28 May)
4.3 Lab 1: Case study on cyber conflict and financial infrastructure under pressure (90 min | 4 June)
4.4 Public-Private partnerships in cybersecurity: working with security agencies and the regulator
4.5 ICT outsourcing and systemic implications of third-party risk
4.6 Supervisory approaches to supply chain and outsourcing risks

Module 5: Artificial Intelligence and the future of cybersecurity

5.1 Live Class 7: AI in financial services (90 mins | 26 May)
5.2 AI as a threat: LLMs, deepfakes, and model manipulation
5.3 Quantum computing and its challenge to encryption methods

Module 6: Strategic simulations and group activities

6.1 Lab 2: Responding to a cyber-geopolitical crisis (90 mins | 18 June)
6.2 Lab 3: Designing responsible and resilient institutions (60 mins | 25 June)

fbf.eui.eu

Co-funded by
the European Union