

EXECUTIVE TRAINING COURSE

PROGRAMME

Managing financial sector cyber risk

Ensuring ICT resilience in an uncertain
geopolitical, AI mediated world

4 May - 26 June 2026

fbf.eui.eu

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

Modules 1 – 3: Digital finance and the cyber threat landscape

Module 1: Digital finance and cyber risk

Module 2: Anatomy of attacks: from phishing to advanced persistent threats

Module 3: Threat actors' ecosystem: from hackers to State-backed operations

Modules 4 – 6: Foundations of cyber resilience

Module 4: Principles of ICT risk management

Module 5: Cybersecurity deep-dive: understanding cyber threat intelligence

Module 6: Cyber crisis communication and managing reputational risk

Modules 7 – 9: Governance, global standards and regulatory frameworks

Module 7: Global standards and cyber governance basics

Module 8: The EU regulatory landscape

Module 9: Lessons in cyber governance from financial authorities

Modules 10 – 15: The geopolitics and geoeconomics of cyberspace

Module 10: The cyber-geopolitical order: systemic risks, sovereignty, and financial stability

Module 11: The new digital battlefield

Module 12: Lab 1: case study on cyber conflict and financial infrastructure under pressure

Module 13: Public-Private partnerships in cybersecurity: working with security agencies and the regulator

Module 14: ICT outsourcing and systemic implications of third-party risk

Module 15: Supervisory approaches to supply chain and outsourcing risks

Modules 16 – 18: Artificial Intelligence and the future of cybersecurity

Module 16: AI in financial services

Module 17: AI as a threat: LLMs, deepfakes, and model manipulation

Module 18: Quantum computing and its challenge to encryption methods

Modules 19 – 20: Strategic simulations and group activities

Module 19: Lab 2: Responding to a cyber-geopolitical crisis

Module 20: Lab 3: Designing responsible and resilient institutions



fbf.eui.eu



Co-funded by
the European Union