COURSE BROCHURE

Cyber Risk Management

An advanced course on identifying cyber risks, estimating them with basic quantitative methods, building a cyber risk register, managing third-party risk and reporting to the board.

Code	HT-IT-109
Category	IT & Cybersecurity
Duration	1 week
Level	Advanced
City	Amsterdam

Introduction

A phrase such as "high breach risk" does not help a board choose between two investments. The decision needs clear scenarios and estimates of possible loss expressed as ranges, however approximate they are.

Objectives

- Write cyber risk scenarios tied to specific assets and processes
- Build a cyber risk register linking each risk to controls, an owner and residual risk
- Estimate event frequency and loss magnitude as ranges using basic quantitative methods
- Assess and monitor the cyber risk posed by suppliers and other third parties
- Present cyber risk to the board in clear financial terms

Who should attend

- Cyber risk and information security managers
- Enterprise risk managers responsible for technology risk
- Supplier risk and technology contracting officers
- Risk advisers who prepare risk reports for board committees

Skills you will develop

- Cyber risk scenario writing
- Quantitative risk estimation
- Third-party risk assessment
- Board risk reporting

Learning Outcomes

- Prepare a cyber risk register for ten scenarios with controls, owners and residual risk
- Estimate the annual loss range for one scenario and present its loss exceedance curve
- Design a supplier tiering model by cyber risk level with the assessment requirements for each tier
- Prepare a two-page board report on the top cyber risks and the options for treating them

Course Outline

Day 1: Cyber Risk in the Organizational Context

- Linking cyber risk to the enterprise risk framework and approved risk appetite

- How assets, threats, vulnerabilities and impact relate
- Identifying risks through scenarios that start from critical processes

Day 2: The Cyber Risk Register

- Writing a clear risk statement with cause, event and impact
- Inherent and residual risk and mapping controls to NIST CSF 2.0 categories
- Ownership, risk acceptance decisions and keeping the register current

Day 3: Basics of Quantification

- The limits of qualitative heat maps and when quantification helps
- Estimating event frequency and loss magnitude as ranges with calibrated expert estimates
- Simple Monte Carlo simulation and the loss exceedance curve

Day 4: Third-Party Cyber Risk

- Tiering suppliers by access to data and systems and by service criticality
- Due diligence questionnaires, the evidence to request and security contract clauses
- Ongoing monitoring and concentration risk with cloud service providers

Day 5: Treatment and Board Reporting

- Treatment options, weighing control cost against expected loss, and cyber insurance considerations
- Key risk indicators and designing the board report
- Applied project: a board report on the top cyber scenarios for the participant's organization, estimated as ranges with treatment recommendations

Training methodology

A workshop drafting risk scenarios from participants' own critical processes
Calibration exercises in which participants test how accurate their ranges are
Running a prepared Excel model for a Monte Carlo simulation of a specific scenario
Presenting the risk report to a simulated risk committee asking board-level questions

Certification

Participants receive a Harbor Training Center certificate of attendance on completing the course.

Upcoming dates

City	Dates	Language	Fee
Amsterdam	8 – 12 February 2027	EN	EUR 6,100
Amsterdam	9 – 13 August 2027	AR	EUR 6,100

Fees are per participant.

Contact us

Email info@harbor4training.com

Address istanbul Turkey

To register and for details, scan the code or visit:

https://harbor4training.com/en/courses/cyber-risk-management