FCAP – FINSEC CYBER ASSESSMENT PROFESSIONAL
TRAINING COURSE

CYBERRISK
INTERNATIONAL
ASSESS | DESIGN | TRANSFORM | SUSTAIN

COURSE DETAILS

This two day boot camp style course has been specifically developed in order to train delegates on how to perform a non technical cyber assessment on a financial institution inline with regulatory cyber compliance requirements.

Objective

This course is delivered by highly experienced financial service experts on cyber regulatory compliance. The objective of the course is to furnish the delegates with the knowledge they require so that they can perform a non technical cyber assessment upon their own organisations, gather the appropriate artefacts and produce the essential level of reporting and assurance for the regulator.

Delegates will also learn how to understand, assess and gain assurance from vendors and partners on third party cyber risk and compliance levels.

Typical Delegates Include:

- Security Professionals
- Compliance personnel
- Risk Managers
- Information Officers
- IT Professionals

Instructors

Paul C Dwyer

CEO of Cyber Risk International and President of the International Cyber Threat Task Force.

Find out more

David Dwyer

Director of Client Services at Cyber Risk International

Find out more

Syllabus

Day One

Module 1
Why Perform a Cyber Assessment?

- Assume Breach
- Legislation
- Assets and Impacts
- Natural Threats
- Cyber Adversarial Risk

Module 2
Cyber Security Fundamental Requirements

- Security v Risk Management v Compliance
- Cyber Security Strategy and Framework
- Governance
- Risk and Control Assessment
- Monitoring
- Response
- Recovery
- Information Sharing
- Continuous Learning
- Additional Localised Cross Industry Requirements

Module 3
Scoping and Planning The Assessment

- Understanding Your Cyber DNA
- Converged Security – Holistic Approach
- Business Strategy
- Identifying Assets
- Key Stakeholders
- Internal Audit
- Third Parties
- Key Business Processes
- People, Processes, Technology
- Jurisdictions
- GRC Requirements
- Industry Compliance Requirements
- Evidence Required
- Planning
- Fieldwork and Documentation
- Issue Discovery and Validation
- Leveraging RegTech

Module 4
Starting The Audit

- Dealing with management, techies and users
- Understanding culture and policy
- Logical and physical
- Assurance and validation

Day Two

Module 5
Inherent Risk Assessment

- Assessing Your Cyber DNA
- Organisational Characteristics
- Delivery Channels
- Online/Mobile Technology Products and Services
- External Threats
- Technologies and Connection Types

Module 6
Cyber Maturity Assessment

- Relationship between Inherent Risk and Cyber Maturity
- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cyber Security Controls
- External Dependency Management
- Cyber Incident Management and Resilience

Module 7
Preparing a Cyber Assessment Report

- Regulator Report Requirements
- Board Level Briefings
- Communicating Results
- Executive Summary
- Cyber Inherent Risk Status
- Cyber Maturity Status
- Roadmap to Maturity
- Cross Map to International Standards and Framework
- Evidence Collected

Module 8
Developing a Framework and Strategy

- Develop a Roadmap to Maturity
- Collect Evidence
- Collaborate and Leverage
- Prove it
- Continually Assessment
- Measuring Improvement
- Next Steps

Get in Touch

For further information please contact us on details below:

+353-(0)1 905 3260
ireland@cri.ie

Global Risk AWARDS 2016

HM Government G-Cloud Supplier APPROVED

www.cyberrisk.ie

CYBERRISK INTERNATIONAL
ASSESS | DESIGN | TRANSFORM | SUSTAIN