INTERNATIONAL CYBER THREAT TASK FORCE
ICTTF

CERTIFIED CYBER RISK OFFICER

CCRO

ONLINE COURSE

In Association with Our Certification Partners

ICA INTERNATIONAL COMPLIANCE ASSOCIATION

CONTENTS

ABOUT THE ICTTF

The ICTTF – International Cyber Threat Task Force was established in 2010 as a not for profit initiative promoting the ecosystem of an international independent non-partisan cyber security community. We have been committed to fostering collaboration, networking and knowledge sharing for almost ten years now.

Over that decade, we have constantly innovated on how best to achieve our mission. From online community portals, apps, local membership chapters and international events we have strived to work with our thousands of members from around the world.

Our mantra is "**It Takes a Network to Defeat a Network**" and our primary objective to foster collaboration and networking has been immensely successful, with our events culminating every year with our annual EU Cyber Summit.

The "bad guys" are strong, highly organised and well trained. Knowledge is power and power is strength. The ICTTF was born in Ireland and when launched used the slogan "Ní neart go cur le chéile" which in English translates to "**There is no Strength Without Unity**". To be strong we all need knowledge and that is why we have developed this online training academy, so organisations can get their staff cyber strong and unified.

We will continue to work with our cadre of global cyber security, risk and privacy experts to develop the worlds best cyber academy. Our first offering is our "Certified Cyber Risk Officer" course and is designed as a non-technical syllabus for business leaders.

ABOUT THIS COURSE

The Cyber Risk Officer course equips students with a comprehensive understanding of cyber risk management. The syllabus assumes a non-technical student and covers a range of topics from identification of cyber risks through to risk management options. The course has been designed to equip students with the knowledge, skills and confidence they require in order to protect the digital assets of their organisation and support the efforts of or lead the implementation of a cyber risk framework

8 Weeks + 1 week initial orientation
New Modules Every Thursday

8-10 Hours Per Week
Self Paced Entirely Online

€1,950
Excluding Taxes

CPE/CPD Points Available
Approved by Various Bodies

Certification
Continual Assessments

Online Academy
Delivered Entirely Online

THE COURSE COVERS

This course brings you on a journey and commences with how to analyse the inherent cyber risk of your organisation. That includes areas such as:

- Organisational Characteristics
- Governance Structure
- Technology Structure and Systems
- Product / Service Delivery Channels
- External Cyber Threats

We then gain an understanding of the current cyber risk status of the organisation holistically by exploring key control areas such as:

- Cyber Risk Management and Oversight
- Cyber Incident Management and Resilience
- Cybersecurity Controls
- Threat Intelligence and Collaboration
- External Dependency – Vendor / Partner Risk

There is a focus on CRQ (Cyber Risk Quantification), meaningful metrics and how to support and develop a cyber strategy that supports your ERM (Enterprise Risk Management) program and business strategy. Security standards, legal and compliance requirements are addressed throughout the material. By the end of the course you will have gained the appropriate knowledge to build, implement or support a risk management framework for your organisation.

THE COURSE IS FOR

The course syllabus has been specifically designed to be collaborative and bring together business leaders of various disciplines within an organisation. They are the key stakeholders in designing, implementing or supporting the cyber risk management program of an organisation. Key cyber risk management stakeholders include:

+ **C-Suite**
+ **CISO/CSO/CIO or CRO**
+ **Head of IT/Security**
+ **CCO Chief Compliance Officer**
+ **Cyber Security/Risk/Compliance Teams**
+ **Legal**
+ **Procurement**
+ **Head of Business Units**
+ **Technology Leaders / Project Managers**
+ **Management Professionals / Team Leaders**
+ **Digital Consultants**

IDEAL TRAINING COURSE FOR

Cyber Risk Leader

Develop and Implement Strategy

Cyber Security and Risk Teams

Collaborate and Support Enterprise

Gaining Recognition

Cyber Risk Management Specialist

HOW DO YOU LEARN

CYBER RISK ACADEMY | ONLINE PORTAL

The course is delivered over 8 weeks and preceded with an orientation module. Every Thursday a new module is added to the course.

During the orientation module you will be introduced to your online teaching and technical support network and gain an understanding of the interface and tools.

During the orientation phase you complete your student profile and gain an understanding of key milestones and how your assessments are calculated.

Training material comprises of rich interactive media such as videos, infographics, activities and course notes. There are many opportunities for collaborative learning via the discussion forums and you can leverage the portal to connect to other students around the world.

During the course you can reference the case study example outlined in Module 1 or reference your own organisation.

During the course students will develop a cyber strategy as part of their assessment, this can be based on their own organisation, the case study or a fictitious entity

YOUR SUPPORT

HIGH LEVEL OF SUPPORT | KEY TO SUCCESS

Head Tutor
Subject Expert

Course Manager
One to One Student Support

Technical Support
Available to Solve Tech Issues

Social Learning
Student Network Collaboration

Extended Network of Material
Recommended External Material

Subtitles/CC
Core Module Videos Have Captions

MODULE 1

Understanding Cyber Risks and a Little Technology

We explore the cyber threat landscape and gain an understanding of the key threat actors, their motivations and techniques. We review a number of high profile cyber attacks with a view to understanding why they were attacked and what could have been done to prevent the breach. We outline a key "Case Study" example that is referenced through the rest of the course.

MODULE 2

Cyber Strategy the Business Case

We outline the importance and the anatomy of a cyber strategy. How a cyber risk framework operates and how it integrates with the organisation. Understand the differences between standards, policies, procedures, legal and regulatory controls. We outline how to identify the business value chain of an organisation and the importance of business systems, assets and entities that support that channel.

MODULE 3

Cyber Risk Quantification and Metrics

We explore the traditional cyber metrics organisations leverage in relation to cyber security and risk and discuss “Meaningful Metrics” that empower the business. Calculating inherent cyber risk, residual cyber risk and aligning those metrics with business objectives. Informing and supporting the business with KPI’s (Key Performance Indicators) and KRI’s (Key Risk Indicators). Leveraging those metrics to develop appropriate maturity roadmaps and report and alert the business.

MODULE 4

Cyber Leadership And Culture

The role of leadership, the governance structure and supporting processes are outlined. The challenge of resourcing, attracting new and developing in-house talent. Establishing a culture of loyalty and business protection. Identifying gaps in leadership and supporting a meritocracy based on talent and ability. Converging the physical security efforts with cyber to deliver a holistic program of protection for your organisation.

MODULE 5

Cyber Risk And The Law

Understanding the complex myriad of cyber related laws, regulations and business requirements is a challenge. In this module, we outline the international landscape of key laws and regulations including GDPR and the NIS Directive. Developing an approach to understanding how to identify what is relevant and may impact your current or future business model. We outline key approaches to identifying the nexus of control requirements and driving efficiency by aligning business, legal and regulatory drivers with business drivers.

MODULE 6

Cyber Resilience And Incident Management

We outline the minimum expectations of regulators when it comes to establishing cyber resilience. Understanding preventative, detective and responsive controls. Best practices in aligning business continuity, disaster recovery and incident response with a program of cyber resilience. We outline the appropriate response to a breach. We focus on key aspects such as detection, communication and containment. We leverage the case study to outline the key aspects and learning points such as proactive strategies to detect an incident and containment strategies to mitigate the impact.

MODULE 7

Third Party Cyber Risk – Vendors and Remote Workers

Every business is comprised of a business value chain. That is the various “links” or parts of the business that support the delivery of a particular service or channel. These links are often provided by third party partners, vendors or remote workers. We explore, how to identify, analyse, manage and report the associated risk to the business. The impact of the paradigm shift in the legal landscape including GDPR and how that factors into your approach.

MODULE 8

Putting It Together – Develop A Cyber Risk Strategy

In this module, we outline how to put everything you have learned together. Students leverage the case study or their own organisations to develop a complete cyber risk strategy. Dissecting the Cyber DNA of the business, establishing key metrics and a maturity roadmap. Aligning with the business strategy and establishing a board level reporting process. Developing processes to measure and manage the implementation of the cyber risk strategy and report the RoI to the business.

HEAD TUTOR

Paul C Dwyer – President of the ICTTF International Cyber Threat Task Force

Paul has been certified an industry professional by the International Information Security Certification Consortium *(ISC2)* and the Information System Audit and Control Association (ISACA) and selected for the IT Governance Expert Panel.

Paul is an honorary fellow of the Irish Computer Society (*ICS*), approved by the National Crime Faculty and the High Tech Crime Network (*HTCN*).

Paul has worked extensively around the world and his diverse career spans more than 25 years working with military, law enforcement, and the commercial sector. His roles have included:

- **President of the International Cyber Threat Task Force** *(ICTTF)*
- **Co Chairman of the UK National Crime Agency** *(NCA)* **Industry Group**
- **Advisor to National Counter Terrorism Security Office** *(NaCTSO)*
- **Advisor to NATO on Countering Hybrid Cyber Threats**
- **Advisor to UK Defence Committee** *(DEFCOM)* **in Parliament**
- **Deputy Chair – Organised Crime Task Force Industry Group – NI**
- **Interim Global CISO for numerous multi national organisations**
- **Advisor to numerous governments and intelligence agencies**

“ Be Smart, Upskill During Downtime ”

A prolific contributor to the industry and media, Paul is a professional public speaker and industry evangelist. He has also authored a number of industry works including a book aimed at boards of director entitled – “**The Art of Cyber Risk Oversight**”.

As an industry networker Paul is a member of a number of distinct groups including the Institute of Directors (*IoD*), Institute of International and European Affairs (*IIEA*) and the Institute of Risk Management (*IRM*)

As an accomplished serial entrepreneur he has successfully built a number of security practices in the UK & Ireland and in 2016 was identified by Business and Finance as one of Ireland’s Top 100 CEOs.

Paul started his career as a technical networking specialist, he then specialised, trained and qualified in a number of disciplines including but not limited to ethical hacking, forensics, international management systems, risk management, business continuity, international governance frameworks, financial service regulations, cyber laws and project management.

Paul is a native of Dublin, Ireland, lives there with his wife, daughter and Bernese mountain dog children.

Paul C Dwyer

Head Tutor

“ *I thought this course would be too technical for me not being in IT, but it is very well paced. The learning materials are easy to follow and concise and the forum collaboration and support is great. The course ties in so many factors across the business from board level to teams that give you a really well rounded approach to cyber security and you can see each week how you can apply this in your everyday roles. Highly recommended!!* ”

Samantha Moolman
Compliance Director, MLRO &
DPO - SHH Operations

“ *This is an excellent course full of information and relevant material for any organisation. I have recently completed a Masters in Cyber Security and I would say this CCRO course has been more practical and useful in my day to day role. I would safely say the Head Tutor, Paul C Dwyer knows everything there is to know about managing cyber risk in today's business environment*

Stephen McCormack
Head of IT - Maxol

“ *This is truly an excellent course. The content is well planned and executed, with continuous reinforcement of important themes and teaching methods. The tutor knowledge and experience are invaluable. The interaction with other students proved valuable on aspects of the course and of the broader cyber risk landscape*

Audrey Barrett
DPO - SIPTU

“ *I would highly recommend the CCRO course. It provides a good overview of the issues and risks associated with Cyber Security, without assuming detailed technical knowledge. I have found the course to be very engaging, structured and well taught.* ”

Richard Atterbury -
Head of Cyber, Compliance, Barclays Bank Plc

“ *Over my long career, I have experienced many courses from the perspective of a participant and a lecturer. I can honestly say the CCRO course stands as one of the best courses I have experienced. It is obvious the course has been developed by experts and has been developed primarily around the student, the content and the delivery. While the course is indeed intense, it is by no means overwhelming. Considering the subject matter , the ability to make the course easily digestible is a massive achievement and credit to the team involved. I would highly recommend this course to anyone who wants to understand and demystify the cyber world in which we now operate.* ”

Dr Vince Hughes
CEO, Director - Crime Stoppers Western Australia
& Crime Stoppers International

Book Now

INTERNATIONAL CYBER THREAT TASK FORCE
ICTTF

For further details,
icttf.org

Online Campus
CyberRiskAcademy.org

Tel: **+353 (0)1 - 905 3263**

Our Partners

ICA INTERNATIONAL COMPLIANCE ASSOCIATION