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 10 years now.

Over that decade, we have consistently innovated on how best to achieve our mission. From online community portals, apps, local membership chapters and international events we strive 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 organized, 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**".

Strength comes from knowledge, so we have developed the Cyber Academy as an online training campus for organizations to educate their staff in becoming cyber strong and unified.

We will continue to work with our cadre of global cyber security, risk and privacy experts to develop the world's best cyber academy. Due to popular demand we have developed the **NCSE– NIST Cyber Security Expert** - certification course. The course focuses on how to establish and operationalize a cyber security program based on the NIST Cyber Security Framework.

ABOUT THIS COURSE

The NCSE (*NIST Cyber Security Expert*) certification course has been developed to teach businesses how to establish and operationalize a cyber security program based on the NIST Cyber Security Framework. This non-technical syllabus aimed at business leaders and/or cyber security practitioners has been developed based on a holistic body of knowledge that encompasses a real-life pragmatic approach to understanding the fundamental concepts of cyber risk management and how to leverage the NIST Cyber Security Framework in order to assess, implement and operationalize a cyber security program. No previous cyber security knowledge is assumed, and the course is appropriate for all levels.

10 Weeks Online Course
24/7 Access to All Training Material

6-8 Hours Per Week
Self Paced Entirely Online

€ 2,499
See Website for Special Offers

CPE/CPD Points Available
Approved by Various International Bodies

Certification
Continual Module Related Exams

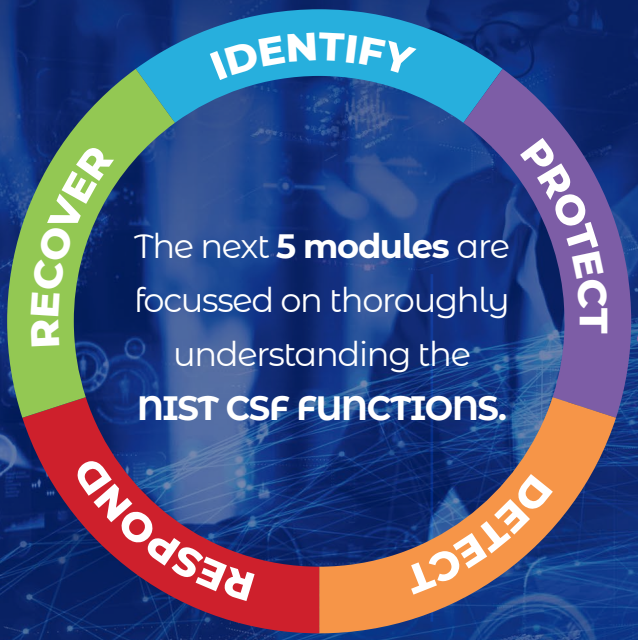
Commences
See Website for Dates

Online Academy
Delivered Entirely Online

THE COURSE COVERS

Course Objective: *"Teaches You How to Establish, Assess and Operationalize a Cyber Security Program Based on the NIST Cyber Security Framework".*

The course is non-technical in approach and supports students on a 10-week journey. You are provided with 24/7 access to all materials and are also supported with access to live learning support sessions. Successful certification is via continual assessments with weekly online exams.



The syllabus presumes little to no cyber related experience, with the first three modules providing an understanding of the basics of cyber security –

- **Cyber Threat Landscape**
- **Cyber Risk Management Fundamentals**
- **Frameworks And Cyber Strategy**

Each function is explained with easy to understand terminology leveraging real-life and abstract examples across each function including every single category and subcategory of controls. We also review the related informative references with implementation tiers for each function area.

Finally, we outline what is involved in **ESTABLISHING A CYBER RISK PROGRAM.** How to apply the **NIST CSF** in the real world is the objective of this the final module.

THE COURSE IS FOR

The course syllabus has been specifically designed to be collaborative and bring together business leaders of various disciplines within an organization. They are the key stakeholders in designing, implementing or supporting the cyber risk management program of an organization. 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 & 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 entirely online. Students are provided with 10 weeks access to all the training material and exams.

Training material comprises of rich interactive media such as videos, infographics 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.

All students also have access to scheduled remote live learning sessions, with an opportunity to directly liaise with the tutor.

There are 10 modules with an online exam at the end of each module. The pass score for each module is 80% and you must obtain an average score of 80% or higher across all modules to be successfully certified.

You can re-sit each of the module exams three times if required during your 10 weeks.

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

MODULES

MODULE 1

Cyber Threat Landscape

We explore the global cyber threat landscape and gain an understanding of the key threat actors, their motivations and techniques. We breakdown the underground economy of cybercrime. We reference real life case studies of high-profile cyber-attacks. This module provides a context and background to the ecosystem of cyber threat actors. We reveal their modus operandi and TTPs (Tactics, Techniques and Procedures) from targeting to money laundering.

MODULE 2

Cyber Risk Management Fundamentals

We explore the key aspects of cyber risk management. Understanding the fundamentals of CRQ (Cyber Risk Quantification) and how to engage the business by leveraging "Meaningful Metrics" related to the business strategy. Developing KPI's (Key Performance Indicators) and KRI's (Key Risk Indicators) that empower the business and how to leverage those metrics to develop appropriate maturity roadmaps and support business leadership in making informed decisions.

MODULE 3

Understanding Frameworks and Cyber Strategy

We outline the importance and the anatomy of a cyber strategy and how a cyber risk framework supports that mission, leadership, culture, governance structure and all supporting processes. We explore how a cyber risk framework operates and how it integrates with the business value chain. Understand the foundational elements including standards, policies, procedures, legal and regulatory controls.

MODULE 4

Anatomy of the NIST Cyber Security Framework

We outline the background and context to the NIST Cyber Security Framework and breakdown the anatomy and structure including functions, categories, subcategories and informative references. We explore the use cases, benefits, future roadmap developments and gain an in-depth understanding of specific terminology and related resources.

MODULE 5

NIST CSF Function | IDENTIFY

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

NIST CSF Function | PROTECT

We explore how to develop and implement appropriate safeguards to ensure delivery of services. We breakdown every single category and subcategory of controls within the “Protect” function. Explained in easy to understand terminology with real-life and abstract examples across the entire NIST CSF function. We explore related informative references and implementation tiers.

MODULES

MODULE 7

NIST CSF Function | DETECT

We explore how to develop and implement appropriate activities to identify the occurrence of a cybersecurity event. We breakdown every single category and subcategory of controls within the "Detect" function. Explained in easy to understand terminology with real-life and abstract examples across the entire NIST CSF function. We explore related informative references and implementation tiers.

MODULE 8

NIST CSF Function | RESPOND

We explore how to develop and implement appropriate activities to take action regarding a detected cybersecurity incident. We breakdown every single category and subcategory of controls within the "Respond" function. Explained in easy to understand terminology with real-life and abstract examples across the entire NIST CSF function. We explore related informative references and implementation tiers.

MODULE 9

NIST CSF Function | RECOVER

We explore how to develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. We breakdown every single category and subcategory of controls within the "Recover" function. Explained in easy to understand terminology with real-life and abstract examples across the entire NIST CSF function. We explore related informative references and implementation tiers.

MODULE 10

Establishing a Cyber Risk Program

Applying the NIST CSF in the real world is the objective of this module. We explore methodologies, protocols and lifecycles in relation to assessing and implementing the framework. We leverage a case study of a financial service entity and walk through assessing the organization, developing a maturity roadmap related to a target profile and implementing it. Understanding how to manage and communicate the status of the program is a key component of this module.

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 – Organized Crime Task Force Industry Group – NI**
- **Interim Global CISO for numerous multi national organizations**
- **Advisor to numerous governments and intelligence agencies**

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.

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 at SHH Operations

This is an excellent course full of information and relevant material for any organization. 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

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

For further details,
icttf.org

Online Campus
CyberRiskAcademy.org

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

Our Partners

ICA International Compliance Association

Technology Ireland ICT Skillnet

ICS The Society for Chartered IT Professionals in Ireland

Crime Stoppers International

Toronto Compliance & AML Events