APPROVED

Institiúid Teicneolaíochta Chorcaí
Cork Institute of Technology

Awards
MSc

Programme Code:	CR_KCYMN_9	**Mode of Delivery:**	Full Time, Fully Online	**No. of Semesters:**	3
NFQ Level:	9				
Embedded Award:	No	**Programme Credits:**	90		
programmeReviewDate:	June 2023				
Department:	COMPUTER SCIENCE				
Field of Study:	Computer Science				

Programme Outcomes

Upon successful completion of this programme the graduate will be able to demonstrate... :

PO1	Knowledge - Breadth	
	(a)	A mastery of the theoretical knowledge and applied skills necessary determine how Cybersecurity governance, risk and compliance enable the alignment of security architecture, engineering and operations to meet business goals. The student will also be able to master other specialist areas of Cybersecurity by taking electives that match their interests.
PO2	Knowledge - Kind	
	(a)	A critical understanding and appraisal of a number of specialist areas in cybersecurity; discuss current challenges and research activities in these areas and apply accepted methodologies for tackling research problems.
PO3	Skill - Range	
	(a)	Evaluate and apply research tools and techniques of inquiry; investigate current challenges in Cybersecurity practice and research; formulate appropriate strategies from emerging theories; communicate to a range of audiences in both written and verbal media cutting edge work in the field of Cybersecurity.
PO4	Skill - Selectivity	
	(a)	Develop the necessary skills to plan and implement a work based project incorporating novel and emerging practices and technologies to develop a solution to a complex problem in Cybersecurity.
PO5	Competence - Context	
	(a)	Analyse and document measures to address risks and weaknesses in Cybersecurity policy and procedures; develop guidelines regarding professional and ethical practices in Cybersecurity; design and implement management frameworks and practices with the aim of improving an organisation's security posture and enhance resilience’s against cyberattacks.
PO6	Competence - Role	
	(a)	Develop the competence required to lead and manage projects in Cybersecurity involving multidisciplinary teams in medium/large organizations; communicate the complexities of Cybersecurity technical project elements to strategic leadership teams in an organisation; Evaluate Cybersecurity risks with the aim of preparing an organisation against likely attacks.
PO7	Competence - Learning to Learn	
	(a)	Develop the knowledge to formulate an appropriate continuing professional development plan based on personal goals. Acquire the knowledge and skills to independently learn and understand Cybersecurity trends to direct new self directed learning and manage the learning pathway of a cybersecurity team.
PO8	Competence - Insight	
	(a)	Expert knowledge in assessing the risk of emerging threats in Cybersecurity and applying governance and management countermeasures in compliance with legal and industry standards to mitigate these threats.

Semester Schedules

Stage 1 / Semester 1

Mandatory	
Module Code	**Module Title**
COMP9079	Security Risk & Compliance
COMP9080	Security Architecture
COMP9081	Security Contingency Planning

Elective	
Module Code	**Module Title**
COMP9053	Scripting for Cybersecurity
MGMT9034	Strategic Thinking
FREE6001	Free Choice Module

Stage 1 / Semester 2

Mandatory	
Module Code	**Module Title**
COMP9082	Security Management and Law
MGMT9063	Communications & Cybersecurity

Group Elective 1	
Module Code	**Module Title**
COMP9084	Security Group Project
COMP9083	Security Work Based Project

Group Elective 2	
Module Code	**Module Title**
COMP9012	Applied Cryptography
MRKT9014	People Management Strategies
COMP9071	Fraud and Anomaly Detection
COMP8063	Emerging Cyber Trends
FREE6001	Free Choice Module

Stage 1 / Semester 3

-

Mandatory	
Module Code	**Module Title**
COMP9021	**Computing Research Project**