

Title	<i>Digital Operational Resilience</i>		
Long Title	<i>Certificate in Digital Operational Resilience</i>		
Author	Gillian O'Carroll		
Awards	Certificate	Embedded Award	No
Programme Code	CR_KDORE_9	Programme Credits	20
Mode of Delivery	Part Time, Fully Online	Programme Review Date	May 2026
No. of Semesters	2	Department	Computer Science
NFQ Level	9		

Programme Outcomes

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

PO1 - Knowledge - Breadth

A critical understanding of the design, development, implementation and evaluation of a range of cybersecurity risk management frameworks and the practical knowledge and skills relevant to apply this knowledge to general cybersecurity risk management, and specifically to digital operational resilience risk.

PO2 - Knowledge - Kind

A mastery of contemporary and upstream cybersecurity and information security regulations, particularly with regards to digital operational resilience, and the critical interplay between various organisational functions and professions.

PO3 - Skill - Range

A critical comprehension of the core cybersecurity risk frameworks and divergent practices that can be utilised in design, implementation and evaluation of a robust Digital Operational Resilience framework.

PO4 - Skill - Selectivity

A broad range of enhanced skills (critical, conceptual, practical and technical) appropriate to an advanced level of professional practice in the field of digital operational resilience, to be evidenced in the content, form, presentational strategies and critical mediation of self-initiated work.

PO5 - Competence - Role

An ability to contribute significantly to, and when appropriate, take a lead role in the design, development, implementation and evaluation of an organisation's Digital Resilience Framework.

PO6 - Competence - Learning to Learn

A critical appreciation of the rapidly changing cybersecurity risk environment, and the need to continuously adapt to this dynamic and rapidly changing environment in order to ensure an organisation demonstrates digital operational resilience.

Semester Schedules

Stage 1 / Semester 1

Mandatory

Module Code	Module Title
CYBR9021	Cybersecurity & DOR

Semester Schedules

Stage 2 / Semester 2

Mandatory

Module Code	Module Title
CYBR9022	Cybersecurity Risk Frameworks