Title	Cybersecurity & DOR
Long Title	Cybersecurity & Digital Op Resilience
Credits	10
NFQ Level	Expert
Module Author	Gillian O'Carroll

Module Description:

In this module, students will evaluate the importance of Digital Operational Resilience as a key component in managing entities' cybersecurity risk environments. The module analyses systemic cyber risks impacting the Digital Economy and provides context for digital operational resilience regulations and standards, such as the EU Digital Operational Resilience Act (DORA) regulatory framework. Key Digital Operational Resilience measures will be appraised, including the ICT Governance Framework, the ICT Risk Management Framework and ICT Third Party Service Providers (including Cloud Computing Service Providers).

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1 Critically appraise the Digital Economy's cybersecurity risk landscape and provide context for Digital Operational Resilience Standards and Frameworks, such as the Digital Operational Resilience Act (DORA) framework.

LO2 Analyse the provisions of Digital Operational Resilience Standards and Frameworks and evaluate how to demonstrate compliance with key components such as ICT Governance Frameworks, ICT Risk Management Frameworks, and ICT Third Party Providers Risk Management requirements.

LO3 Select and apply relevant internationally accepted cybersecurity risk frameworks and consider their relationship with Digital Operational Resilience Standards and Frameworks, including the DORA Regulations.

LO4 Examine the concept of 'Digital Operational Resilience' and identify the essential elements of a comprehensive Testing Programme, including consideration of an evolving cybersecurity risk landscape.

LO5 Investigate both the legal and non-financial implications of non-compliance with Digital Operational Resilience Standards & Frameworks, such as the DORA Regulations. Consider the longer-term impact on financial entities.

Indicative Content

Digital Operational Resilience & Legal Outline

Systemic threats to entities operating in the Digital Economy and the EU's Digital Landscape threat analyses. EU approach to managing crises and building resilience. Legal basis for the EU's Digital Operational Resilience Act (DORA), and its scope and compliance requirements. DORA's link to other relevant legislation, including the Payment Services Directive 2 (PSD2) and the NIS Directives (1 and 2).

Risk Management Frameworks

Key principles of Risk Management and additional considerations for effective cybersecurity risk management. International Cybersecurity Risk Management Frameworks, such as the NIST Cybersecurity Framework and COBIT19, and their relationship to Digital Operational Resilience. Outsourcer/Third Party Risk Management within the context of a comprehensive risk framework.

ICT Governance & ICT Risk Management Frameworks

Concept of 'governance' and its importance for strong risk frameworks. Key elements of an ICT Governance Framework, including documentation of policies and procedures, roles and responsibilities, and budgetary requirements. Key elements of an ICT Risk Management Framework, including appropriate strategies and policies, required ICT systems, protocols and tools, and essential components of a Digital Operational Risk Strategy. Regulators' requirements on operational resilience, such as the Central Bank of Ireland's Cross Industry Guidance on Operational Resilience.

Identification, Protection, Prevention, Detection, Response & Recovery

Risk-based approaches to identifying and monitoring ICT threats and vulnerabilities. Data Management Policies for data risk minimisation for data-in-transit, data-in-use and data-at- rest. ICT Change Management. Prevention and Detection programmes to meet the requirements of Digital Operational Resilience Standards and Frameworks. Testing for Redundant Sites and Replicated Sites. Business Continuity Plans and Response & Recovery Plans as part of a Digital Resilience Strategy.

Learning & Evolving

Post-Incident Reviews. Communication Plans, Policies and Procedures as part of Digital Operational Resilience Strategies. ICT Security Awareness Programmes as an essential element of cyber risk reduction.

Oversight Framework

Legal framework underpinning Digital Operational Resilience Standards & Frameworks, including fines and penalties for non-compliance. Information Sharing proposals and Incident Reporting frameworks. Upstream EU Regulatory Technical Standards and potential impact on the compliance landscape.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Written Report	The Learner will produce a written report to a professional standard analysing the cybersecurity risk landscape for entities operating in the Digital Economy and how compliance with Digital Operational Resilience Standards and Frameworks will impact risk.	1,2,3	40	Week 6
Project	Learners will select a Use-Case/Real Organisation and document a case study on the measures the Use-Case Organisation can take to prepare for compliance with Digital Operational Resilience Standards & Frameworks, such as DORA. Learners must document their research and create a presentation capable of clearly expressing a summary of their findings to their peers and experts in the field.	3,4,5	60	Sem End

Assessment Breakdown

%

Coursework	100

Re-Assessment Requirement

Coursework Only

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture underpinning the learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support content delivered.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	10.0	Every Week	10.00
		Total Hours		14.00
		Total Weekly Learner Workload		14.00
		Total Weekly Contact Hours		4.00

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture underpinning the learning outcomes.	2.0	Every Week	2.0
Lab	Lab to support content delivered.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	10.0	Every Week	10.00
		Total Hours		14.00
		Total Weekly Learner Workload		14.00
		Total Weekly Contact Hours		4.00

Recommended Book Resources

- **US Department of Commerce 2022, *National Institute of Standards & Technology (May 2022), Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* [ISBN: 9798837348969]**