MODULE DESCRIPTOR

Module Title

Information Risk & Security Management

Reference	CM3144	Version	1
Created	November 2023	SCQF Level	SCQF 9
Approved	April 2024	SCQF Points	15
Amended		ECTS Points	7.5

Aims of Module

This module aims to provide students with a thorough comprehension of information risk and security management, empowering them to identify, assess, and manage information security risks effectively within an organizational context.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Demonstrate a comprehensive understanding of various information security risks within organizational settings.
2	Assess the information security risks for a given scenario.
3	Demonstrate a comprehensive understanding of information security management principles.
4	Formulate a cybersecurity program aligned with organisational objectives and relevant regulations.

Indicative Module Content

Risk Definition; Risk Perception Factors; Human Factors and Risk Communication; Security Culture; Information Security Standards; Enacting Security Policy; Component vs. Systems Perspectives; Elements of Risk (e.g., Vulnerability, Threat, Likelihood, Impact); Risk Assessment and Management Methods (e.g., NIST Guidelines, ISO/IEC 27005, Octave Allegro, STRIDE, Attack Trees); Governance Models; Legal and Regulatory Frameworks (e.g. GDPR, Computer Misuse Act, ISO27001, HIPAA,PCI DSS); Audit and Compliance; Information Security Governance and Planning; Information Assurance; Planning for Risk Assessment; Managing Risks and Threats; Information Security Policy Principles; Information Security Policy Implementation; Physical and Environmental Security; Technical Security Controls; Information Sharing; Business Continuity; Incident Response and Recovery Planning (e.g., ISO/IEC 27035, NCSC Guidance); Risk Assessment and Management in Cyber-Physical Systems (OT, ICS, CNI, SCADA, NIS); Security Metrics.

Module Delivery

Key concepts are introduced and illustrated through lectures and directed reading. The understanding of students is tested and further enhanced through lab sessions.

Module Ref:	CM3144 v1

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4
Description:	Coursework consisting of both practical and theoretical elements covering all module learning outcomes.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of Component 1. An overall minimum grade of D is required to pass this module

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1
B	The student needs to achieve a B in Component 1
C	The student needs to achieve a C in Component 1
D	The student needs to achieve a D in Component 1
E	The student needs to achieve an E in Component 1
F	The student needs to achieve an F in Component 1
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CM3144 v1

INDICATIVE BIBLIOGRAPHY

1	Broad, J. (2022). Risk Management Framework: A Lab-Based Approach to Securing Information Systems. Apress.
2	Priyadarshini, I., & Cotton, C. (2022).?Cybersecurity: Ethics, Legal, Risks, and Policies. CRC Press.
3	Hodson, C. J. (2019).?Cyber risk management: Prioritize threats, identify vulnerabilities and apply controls. Kogan Page Publishers.
4	Hubbard, D. W., & Seiersen, R. (2023).?How to measure anything in cybersecurity risk. John Wiley & Sons.
5	Landoll, D. (2021).?The security risk assessment handbook: A complete guide for performing security risk assessments. CRC Press.
6	Sutton D., (2021). Information Risk Management: A practitioner's guide. BCS
7	Gregory, P., (2018). CISM Certified Information Security Manager All-in-One Exam Guide (CERTIFICATION & CAREER - OMG). McGraw Hill.