ROBERT GORDON UNIVERSITY ABERDEEN

This Module Version is Pending Validation

MODULE DESCRIPTOR

Module Title

Maritime Cyber Security

Reference	CM3403	Version	1
Created	November 2023	SCQF Level	SCQF 9
Approved		SCQF Points	15
Amended		ECTS Points	7.5

Aims of Module

To provide students with an understanding of the main security threats to the maritime industry. To develop the students' skills in supporting safe and secure shipping, which is operationally resilient to cyber risks.

Learning Outcomes for Module

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

1	Discuss the main threats to maritime security.
2	Assess maritime cyber risks.
3	Formulate mitigation security measures against maritime cyber risks.
4	Discuss the regulatory framework and its role in maintaining a basic cyber hygiene.

Indicative Module Content

Cyber security fundamentals: security objectives (C.I.A.); vulnerabilities, threats, and risk. Cyber security in the maritime industry: hazards, threat modelling, case studies. Risk assessment and management: Maritime cyber risk assessment; risk management and mitigation; Cyber Security Plan (CSP). Regulatory framework and maritime cyber security guidelines and best practices: The department for transport's Cyber Security Code of Practice for Ships; the International Maritime Organization (IMO) guidelines; The National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF), ISO 27001/2, and the EU's NIS-Directive.

Module Delivery

This module is delivered by self-directed learning, facilitated by formative activities and online tutor support.

Indicative Student Workload	Full Time	Part Time
Contact Hours	20	20
Non-Contact Hours	130	130
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	150
Actual Placement hours for professional, statutory or regulatory body		

Module Ref:	CM3403 v1

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:	A report discussing cyber risks and appraising security mitigations.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of C1. An overall minimum grade D is required to pass the 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.

INDICATIVE BIBLIOGRAPHY

1 The Department for Transport. 2023. Cyber Security Code of Practice for Ships. Online. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1175769/code-of-practice-cyber-security-for-ships.pdf

2 KESSLER, G.C., and SHEPARD, S.D., 2022. Maritime Cybersecurity: A Guide for Leaders and Managers. Independently published. Online. https://www.garykessler.net/MaritimeCybersecurityBook/index.html

3 Drumhiller, N.K., 2017. Issues in Maritime Cyber Security. Westphalia Press.

4 NORMAN, T.L., 2016. Risk analysis and security countermeasure selection. CRC Press.