Module Specification

1. Factual information			
Module title	**MT395: Applied Cyber Security**	**Level**	**3**
Module tutor		**Credit value**	**10**
Module type	**Taught**	**Notional learning hours**	**3**

2. Rationale for the module and its links with other modules

- In today's world, organizations must be prepared to defend against threats in cyberspace. Decision makers must be familiar with the basic principles and best practices of cyber security to best protect their enterprises.

3. Aims of the module

The aims and objectives of this module are to:

- Describe and discuss a range of topics in cyber security management.
- Describe cyber security governance and the implementation of an integrated security mechanism.
- Identify cyber security threats and explain risk analysis and management.
- Allow students to perform independent research in the area and to critically read and analyse third party material.

4. Pre-requisite modules or specified entry requirements

Students should have completed the study of TM260

5. Intended learning outcomes	
A. Knowledge and understanding	**Learning and teaching strategy**
After studying the module you will be able to: **A1.** Describe cyber security fundamentals **A2.** Explain cyber security management and its importance to organizations **A3.** Evaluate the principles of cyber security governance to sustain and improve the security posture of an organisation **A4.** Interpret the importance of risk analysis and management in protecting an organization from cyber threats **A5.** Evaluate cyber security management policies, standards, and processes **A6.** Define the most common cyber security threats and analyse appropriate countermeasures **A7.** Describe and discuss the application of an integrated security mechanism	• 25% face-to-face tutorial sessions • TMA work • Module textbook and support material

B. Cognitive skills	**Learning and teaching strategy**
After studying the module you will be able to: **B1.** Recognise and define the main issues and challenges related to protecting and safeguarding organisations from cyber security risks	• 25% face-to-face tutorial sessions • TMA work • Module textbook and support material

B. Cognitive skills	Learning and teaching strategy
B2. Read, evaluate, and critically review technical documents and extract useful information from these documents on topics related to cyber security, risk management, threat detection and countermeasures	

C. Practical and professional skills	Learning and teaching strategy
After studying the module you will be able to: **C1.** Use the studied concepts to analyse and assess the cyber security risks **C2.** Identify the threats to information security and take appropriate countermeasures	• 25% face-to-face tutorial sessions • TMA work • Module textbook and support material

D Key transferable skills	Learning and teaching strategy
After studying the module you will be able to: **D1.** Demonstrate independent self-learning capabilities in order to tackle more advanced topics and remain up-to-date in the field of cyber security **D2.** Employ your technical writing skills on topics related to cyber security and cyber security management	• 25% face-to-face tutorial sessions • TMA work • Module textbook and support material

6. Indicative content.	
1.	Introduction to Cyber Security
2.	Organizational Strategic Governance Framework
3.	Business Continuity Management Planning Framework
4.	Communication Risk Management Strategy
5.	Risk Assessment Policy and its Strategic Context
6.	Resilience Policy and Strategy Mapping
7.	Integrated Resilience Management Model
8.	Integrated Management Model and System
9.	Integrated Governance Mechanism
10.	Threat Identification
11.	Governance and Compliance Decision Making Process
12.	Integrated Security Mechanism

7. Assessment strategy, assessment methods and their relative weightings
TMA Work: 20% MTA: 30% Exam: 50%

8. Mapping of assessment tasks to learning outcomes													
Assessment tasks	**Learning Outcomes**												
	A1	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**	**B1**	**B2**	**C1**	**C2**	**D1**	**D2**
TMA		✓	✓	✓	✓			✓	✓	✓	✓	✓	✓
MTA	✓	✓	✓	✓									
Final Exam	✓	✓	✓	✓	✓	✓	✓	✓		✓			

9. Teaching staff associated with the module	
Tutor's name and contact details	**Contact hours**
To be appointed at a later date since this is a new module.	

10. Key reading list				
Author	**Year**	**Title**	**Publisher**	**Location**
Peter Trim and Yang-Im Lee	**2014**	**Cyber Security Management: A Governance, Risk and Compliance Framework**	**Gower Publishing**	**UK**
Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies	**2015**	**Security in Computing, 5th Edition**	**Prentice Hall**	

11. Other indicative text (e.g. websites)

- **D. Alexander, A. Finch, and D. Sutton, "Information Security Management Principles", BCS, 2nd Edition, 2013.**
- **Leo Dregier, "Penetration Testing and ethical Hacking", Cybrary, 2009. URL:** https://www.cybrary.it/course/ethical-hacking/
- **Kevin Mitnick and William Simon, "The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders and Deceivers", Wiley, 2005.**