STUDENT AND ACADEMIC SERVICES

MODULE SPECIFICATION

Part 1: Information			
Module Title	Risk and Information Management		
Module Code	UFCFMU-30-3	Level	Level 6
For implementation from	2022-23		
UWE Credit Rating	30	ECTS Credit Rating	15
Faculty	Faculty of Environment & Technology	Field	
Department	FET Dept of Computer Sci & Creative Tech		
Module type:	Standard		
Pre-requisites	Information management and security 2021-22		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

Overview: Risk assessments are used to identify, estimate, and prioritize risk to organisational operations (i.e., mission, functions, image, finance and reputation), organisational assets, individuals and other organisations, resulting from the operation and use of information systems. In order to assess risk, the systems need to be explored for weaknesses, either technical or social. Reconnaissance methods emulate those of attackers.

This module focusses on people and the human factors of cyber security. and examines:

- the methods and roles of those involved in attacking systems
- analysing system weaknesses
- assessing the associated risks and managing them

Educational Aims: This module addresses the human factors in cyber security.

Outline Syllabus: You will cover:

- the role of information security awareness and training
- behavioural analysis and security culture management in maintaining good information security

- the motivations and ways of thinking of different classes of threat actors, criminal intent, activism, state actors, hackers, and how this drives the behaviour of the threat actors
- tailoring mitigations for the different classes of threat actor
- social engineering and phishing
- insider threat
- malicious intent and human error
- usable security
- creation of a reasoned argument employing evidence to support a position
- how threat actors' actions appear in typical sources of information
- sourcing intelligence ethically so that it may be used as required
- methods attackers/threat actors may use to build knowledge of a system they have limited or no direct access to, such as:
- phishing
- exploiting an insider
- port scanning
- open source intelligence
- asset valuation and management concepts
- risk analysis methodologies in common use
- risk appetite and risk tolerance concepts
- economics of security concepts
- different ways of treating risk (mitigate, transfer, accept etc.)
- principles of system risk modelling a system risk modelling methodology
- an enterprise modelling technique such as UML
- risk assessment and risk management methodologies
- approaches to risk treatment (mitigate, transfer, accept, etc.)
- risk management in practice
- examples such as technical, business process, or other
- description of risk in qualitative, quantitative, or mixed terms
- role of risk owner, contrasting role with other stakeholders

Teaching and Learning Methods: Lecture sessions cover the technical knowledge required. Practical sessions allow the students to apply their theoretical knowledge to real and/or case study organisations.

Part 3: Assessment

Assessment 1 – Component A
Apprentices will be provided with a case study of a system (in document and physical form) for them to perform a complete risk assessment. They will submit a notebook of their findings and methods, which will inform a 30 minute oral examination of their work.

In the coursework, students undertake a research-based assignment in which they investigate the (theoretical) roles and actions that people play in cyber security, both beneficial and harmful.

In component A of assessment, they undertake an oral exam in which they use their theoretical findings to inform a risk assessment based on a case study with which are provided. Students are expected to keep a notebook of their findings and methods and to submit this as background to their oral exam.

This assessment also serves as a preparation for an End-Point-Assessment.

First Sit Components	Final Assessment	Element weighting	Description
Case Study - Component A	✓	60 %	Oral examination of a risk assessment based on a case study and supported by notes taken during the development of the the risk assessment.
Report - Component B		40 %	Report of research into the roles and behaviours that impact human factors in cyber security.

Resit Components	Final Assessment	Element weighting	Description
Case Study - Component A	✓	60 %	Oral examination of a reworked risk assessment based on a case study and supported by notes taken during the risk assessment process.
Report - Component B		40 %	Reworked report

Part 4: Teaching and Learning Methods

Learning Outcomes

On successful completion of this module students will achieve the following learning outcomes:

Module Learning Outcomes	Reference
Demonstrates systematic understanding of human dimensions of cyber security.	MO1
Apply structured and ethical intelligence analysis, methods, techniques.	MO2
Perform risk modelling, analysis, identifying and responding to contemporary cyber threat trends.	MO3
Perform risk assessment to an external standard.	MO4

Contact Hours

Independent Study Hours:	
Independent study/self-guided study	135
Total Independent Study Hours:	135
Placement Study Hours:	
Placement	75
Total Placement Study Hours:	75
Scheduled Learning and Teaching Hours:	
Face-to-face learning	90
Total Scheduled Learning and Teaching Hours:	90
Hours to be allocated	300
Allocated Hours	300

Reading List

The reading list for this module can be accessed via the following link:

	https://rl.talis.com/3/uwe/lists/F434F272-1DFF-02C5-4E0C-B604B66633BE.html

Part 5: Contributes Towards
This module contributes towards the following programmes of study: BSc (Hons) Cyber Security Technical Professional (integrated degree) BSc (Hons) 2020-21