# Module Specification

## Risk and Information Management

Version: 2023-24, v2.0, 19 Jul 2023

**Contents**

## Part 1: Information

**Module title:** Risk and Information Management

**Module code:** UFCFMU-30-3

**Level:** Level 6

**For implementation from:** 2023-24

**UWE credit rating:** 30

**ECTS credit rating:** 15

**Faculty:** Faculty of Environment & Technology

**Department:** FET Dept of Computer Sci & Creative Tech

**Partner institutions:** None

**Field:**

**Module type:** Module

**Pre-requisites:** Information management and security 2022-23

**Excluded combinations:** None

**Co-requisites:** None

**Continuing professional development:** No

**Professional, statutory or regulatory body 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

**Features:** Not applicable

**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

## Part 3: Teaching and learning methods

**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.

**Module Learning outcomes:** On successful completion of this module students will achieve the following learning outcomes.

**MO1** Demonstrates systematic understanding of human dimensions of cyber security.

**MO2** Apply structured and ethical intelligence analysis, methods, techniques.

**MO3** Perform risk modelling, analysis, identifying and responding to contemporary cyber threat trends.

**MO4** Perform risk assessment to an external standard.

**Hours to be allocated:** 300

**Contact hours:**

Independent study/self-guided study = 135 hours

Placement = 75 hours

Face-to-face learning = 90 hours

Total = 300

**Reading list:** The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/F434F272-1DFF-02C5-4E0C-B604B66633BE.html

## Part 4: Assessment

**Assessment strategy:** 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.

Students will also 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.

The oral exam explores their use of theoretical findings to inform a risk assessment based on a case study with which are provided. The submitted notebook acts as background to their oral exam.

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

**Assessment tasks:**

**Case Study** (First Sit)
Description: Oral examination of a risk assessment based on a case study and supported by notes taken during the development of the the risk assessment.
Weighting: 60 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO3, MO4

**Report** (First Sit)

Description: Report of research into the roles and behaviours that impact human factors in cyber security.
Weighting: 40 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2

**Case Study** (Resit)
Description: Oral examination of a risk assessment based on a case study and supported by notes taken during the development of the the risk assessment.
Weighting: 60 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO3, MO4

**Report** (Resit)
Description: Report of research into the roles and behaviours that impact human factors in cyber security.
Weighting: 40 %
Final assessment: No
Group work: No
Learning outcomes tested: MO1, MO2

## Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security Technical Professional {Apprenticeship-GLOSCOLL}
[Sep][FT][GlosColl][3yrs] BSc (Hons) 2021-22