STUDENT AND ACADEMIC SERVICES

MODULE SPECIFICATION

Part 1: Information

Module Title	Information Risk Management		
Module Code	UFCFWN-15-M	Level	Level 7
For implementation from	2019-20		
UWE Credit Rating	15	ECTS Credit Rating	7.5
Faculty	Faculty of Environment & Technology	Field	Computer Science and Creative Technologies
Department	FET Dept of Computer Sci & Creative Tech		
Module type:	Standard		
Pre-requisites	None		
Excluded Combinations	None		
Co- requisites	None		
Module Entry requirements	None		

Part 2: Description

Overview: For all organisations, the need for recognising effective methods of information security management is paramount. With the technological advances in the workplace, businesses face new threats and vulnerabilities that have not previously been considered, such as recent cyber-attacks in the forms of phishing campaigns, denial of service, and ransomware.

In this module, we study the roles of information security management and information risk management.

Educational Aims: See Learning Outcomes.

Outline Syllabus: We look to understand the current landscape that businesses are faced with via real-world case studies and study these in the context of the information security CIA triad (confidentiality, integrity, availability). We introduce the terminology of threats, vulnerabilities, impact, and risk, to assess the likelihood and severity of security incidents.
We consider the scope of external threats, such as global malware infection and political conflict, and also focus on insider threats, such as data theft or sabotage by those acting within the organisation, and discuss how such cases can be managed. We also examine how the International Organization for Standardization can facilitate the identification, analyse, and mitigation of risks. We consider in detail the information security management frameworks that are in the ISO 27000 family, to support the development of an Information Security Management

System (ISMS). We also make use of the British Standards Institute to study related ISO documentation for risk management, include ISO 9000 and ISO 31000. We also study the relevant legislation, regulations, policy, that relate to information security, including the Computer Misuse Act, the Data Protection Act, and the more recent General Data Protection Regulation, to understand how this can protect individuals and businesses from the potential threats that exist.

Teaching and Learning Methods: The course is taught through weekly one-hour lectures, with weekly two-hour seminar discussions. Whilst the core course content is delivered via lectures, the seminars then facilitate the discussion of real- world news stories and security incidents related to the process of risk identification and risk mitigation.

Part 3: Assessment

The assessment of this module consists of two components (A and B):

A. 15-minute presentation to disseminate the findings reported in Component B, providing the opportunity to expand on the report, and addressing the role of the Information Security Management System and how this could be implemented in the reported context to mitigate future incidents.

B. 3000-word report that provides a critical reflection on a real- world security incident, which also proposes how the adoption of an Information Security Management System could facilitate possible mitigation, and which identifies and discusses other forms of security incidents which may be relevant to the organisation in the future.

First Sit Components	**Final Assessment**	**Element weighting**	**Description**
Report - Component B		75 %	3000 word report providing a critical reflection on a real-world security breach
Presentation - Component A	✓	25 %	Individual presentation (15 minutes)
Resit Components	**Final Assessment**	**Element weighting**	**Description**
Report - Component B		75 %	3000 word report providing a critical reflection on a real-world security breach
Presentation - Component A	✓	25 %	Individual presentation (15 minutes)

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
Form deep and systematic understanding of relevant standards, such as ISO27001, in the context of Information Security Management	MO1
Analyse a broad range of real-world security issues that face commercial organisations and other institutions	MO2
Evaluate and critique the shortcomings of real-world security incidents, and provide clear justification and innovation solutions for how ISMS could help mitigate future incidents	MO3
Assess and evaluate the appropriateness of security laws and regulations	MO4
Reflect on personal capabilities for the proposal of an ISMS, providing a strong rationale for the methods adopted	MO5

Contact Hours	**Independent Study Hours:**	
	Independent study/self-guided study	114
	Total Independent Study Hours:	114
	Scheduled Learning and Teaching Hours:	
	Face-to-face learning	36
	Total Scheduled Learning and Teaching Hours:	36
	Hours to be allocated	150
	Allocated Hours	150
Reading List	*The reading list for this module can be accessed via the following link:* https://uwe.rl.talis.com/modules/ufcfwn-15-m.html	

Part 5: Contributes Towards

This module contributes towards the following programmes of study: