STUDENT AND ACADEMIC SERVICES

MODULE SPECIFICATION

Part 1: Basic Data

Module Title	Information Security		
Module Code	UFCFHJ-15-M	Level	M
UWE Credit Rating	15	ECTS Credit Rating	7.5
Owning Faculty	FET	Field	Computer Science and Creative Technologies
Department	Computer Science and Creative Technologies	Module Type	Standard
Contributes towards	MSc in Information Technology MSc Financial Technology		
Pre-requisites	None	Co- requisites	None
Excluded Combinations	None	Module Entry requirements	
First CAP Approval Date	November 2015	Valid from	Sept 2016
Revision Approval Date	CAP June 2016 v1.1 UVP 29 May 2019 v2	Revised with effect from	September 2016 September 2019

Part 2: Learning and Teaching

Learning Outcomes

On successful completion of this module students will be able to:

	Assessed in component
1. Synthesise and evaluate key information security principles, risks, threats and vulnerabilities faced by public or private organisations	A
2. Analyse information security issues related to privacy, civil liberties and intellectual property, reporting at board level	B
3. Propose a standards compliant information security framework and/or policy suited for consideration by a public or private organisation board	B
4. Apply a recognised information security standard to prescribe technical controls appropriate for a public or private organisation	A
5. Collaborate as a team to research and communicate a critique of current/emerging information security trends to technical and non-technical audiences	B

Syllabus Outline

- Foundational: information security principles, information risk; threats and vulnerabilities
- Key information security issues: regulation; privacy; civil liberties; intellectual property and cybercrime
- Information security management: ethics; frameworks and policies; secure software development; physical and environmental security; disaster recovery and business continuity management
- Technical information security controls: authentication and authorisation; data security; network security; computer security; application security
- Information security trends: governance; identity and access management;

mobile and cloud security

Contact Hours

Module contact time consists of 24 hours of lectures and seminars/tutorials.

Additionally, students should expect to spend a considerable amount of time (~86 hours) in independent study, including time spent in directed reading, assimilating the material presented during contact hours and working within groups.

Teaching and Learning Methods

The core module content is introduced through lectures. All teaching and learning activities (both scheduled and independent) are aligned with the learning outcomes. Tutorials and seminars aim to reinforce and extend the material delivered in the lectures.

Independent learning requires students to spend time in directed reading, developing research skills and in collaboration with other students in order to assimilate material presented during the contact hours to develop this further for the group assignment.

This 15 credit module requires (notionally) 150 hours of study. The module delivery is organised as follows:

Activity	**Hours**
Contact time • 25% for lectures, tutorials, seminars and tutor-led activities	24
Assimilation and development of knowledge • 50% for independent learning, both individually and within groups	86
Assessment • 25% examination and 75% coursework, which approximately equates to: ○ Exam preparation ~6% (10 hours) reviewing selected module content against examined learning outcomes ○ Coursework preparation ~19% (30 hours) preparing group coursework for assessment	40
Total study time	**150**

The teaching and learning strategy enabling the examination is:

- Scheduled learning
  - Lectures – introduces topics (relevant to learning outcomes 1 and 4) to be assessed
  - Tutorials/Seminars – tutor-led teaching and learning activities to deepen the topic(s) covered
- Independent learning
  - Directed reading – self-managed study to review and deepen directed topics
  - Group collaboration – student-student interaction to elaborate, reflect and apply topics
- Examination preparation
  - Tutor guidance – revision session/advice
  - Self-directed review of topics addressing learning outcomes 1 and 4, as covered during lectures

The teaching and learning strategy enabling the group assignment is:

- Scheduled learning
  - Lectures – introduce some topics (relevant to learning outcomes 2, 3 and 5) that may be chosen by the group for use in the assessment

	o Tutorials/Seminars – tutor-led teaching and learning activities to extend and deepen the topic(s) covered. Formative feedback is offered • Independent learning o Directed reading – self-managed study to review, deepen and extend directed topics knowledge and understanding o Group collaboration – student-student interaction to research, elaborate, reflect and apply group chosen topics • Assignment preparation o Tutor guidance – group assignment advice o Self-directed group review of assignment against learning outcomes 2, 3 and 5
Reading Strategy	**Core reading** Students should will be directed to the relevant sections of a range of texts. In addition students are also required to read supplementary material available through the Library, Blackboard, the Internet and suggested by the tutor. A range of research papers and online readings will be supplied. Full text access to relevant information security standards will be provided. **Further reading** Individual module topics will have tutor-supplied lists of online reading and audio/video media. In addition, links to online resources to support study and research skills necessary for the module will be provided. Students are expected to identify additional reading relevant to current/emerging information security trends for themselves. They will be required to read widely using the library search, bibliographic and full text searches, and Internet resources. The purpose of this further reading is to ensure that students are familiar with foundational principles, current research and emerging trends. **Access and skills** The development of literature searching skills is supported by a Library seminar provided within the first semester. Students will be presented with further opportunities within the curriculum to develop their information retrieval and evaluation skills in order to identify such resources effectively. Additional support is available through the library web pages, including interactive tutorials on finding books and journals, evaluating information and referencing. Sign up workshops are also offered by the Library.
Indicative Reading List	The following list is offered to provide validation panels/accrediting bodies with an indication of the type and level of information students may be expected to consult. As such, its currency may wane during the life span of the module specification. However, as indicated above, *current* advice on readings will be available via the module handbook. Shimeall, T. and Spring, J. (2014). *Introduction to information security*. Waltham MA: Elsevier (Set text for the module) Singer, P. and Friedman, A. (2014.). *Cybersecurity and cyberwar*. Oxford: Open University Press Whitman, M. and Mattord, H. (2015). *Principles of information security,* 5th edn. Boston: Cengage

Part 3: Assessment	
Assessment Strategy	The assessment strategy has been selected to enable students to demonstrate a rich understanding of the facets of information security and the correct selection and application of controls across a range of contexts . (assessed via exam). Credit will be given for students who illustrate wider reading and understanding through the selection of appropriate examples and case studies Secondly, through a group assignment, students will develop the ability to work in a team to analyse trends and legislative environment and develop standards-compliant policies – the results of which can be communicated professionally at senior management level in written form, suitably structured and annotated. **Examination (25%)** Learning outcomes 1 (explaining key information security risk, threats etc) and 4 (outlining technical controls) are assessed by a short-answer, controlled-conditions, 1.5 hour examination. **Group Assignment (75%)** Learning outcomes 2 (analysing privacy, civil liberties and intellectual property), 3 (proposing standards–compliant framework/policy) and 5 (collaborating to critique information security trends) are assessed by a group coursework. Two key dimensions of the group assignment will be assessed: • The *product* produced by the group • The group *collaboration process*, including the skills and effort put in by members of the group in creating the product The product will be marked using detailed assessment criteria (published within the assignment brief). The collaboration process will use distinct assessment criteria. This will apply peer assessment of the group collaboration process to create an *individual process weighting factor*. The individual weighting factor will determine the proportion of the product mark awarded to an individual student. Students will be instructed to adopt UWE advice and policies on study skills, Harvard Referencing and word count. The assignment length will be around 3,000 words.

Identify final assessment component and element	***Comp A***	
% weighting between components A and B (Standard modules only)	**A:** **25%**	**B**: **75%**
First Sit		
Component A (controlled conditions) **Description of each element**	**Element weighting** **(as % of component)**	
1. Unseen examination (1.5 hours)	100%	
Component B **Description of each element**	**Element weighting** **(as % of component)**	
1. Group assignment – product report (3,000 words)	100%	

Resit (further attendance at taught classes is not required)	
Component A (controlled conditions) **Description of each element**	**Element weighting** **(as % of component)**
1. Unseen examination (1.5 hours)	100%
Component B **Description of each element**	**Element weighting** **(as % of component)**
1. Individual report (3,000 words)	100%