Module Specification

Information Risk Management

Version: 2023-24, v2.0, 27 Jul 2023

Contents

Part 1: Information

Module title: Information Risk Management

Module code: UFCFWN-15-M

Level: Level 7

For implementation from: 2023-24

UWE credit rating: 15

ECTS credit rating: 7.5

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body 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.

Features: Not applicable

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.

Part 3: Teaching and learning methods

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.

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

MO1 Form deep and systematic understanding of relevant standards, such as ISO27001, in the context of Information Security Management

MO2 Analyse a broad range of real-world security issues that face commercial organisations and other institutions

MO3 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

MO4 Assess and evaluate the appropriateness of security laws and regulations

MO5 Reflect on personal capabilities for the proposal of an ISMS, providing a strong rationale for the methods adopted

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Total = 150

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/modules/ufcfwn-15-m.html

Part 4: Assessment

Assessment strategy: This module consists of one assessment.

A 30-minute group presentation to provides a critical reflection on a real- world security incident, which also proposes how the adoption of an Information Security Management System and how this could be implemented to mitigate future incidents.

The resit assessment follows the same format as the first sit.

Assessment tasks:

Presentation (First Sit)
Description: Group presentation (30 minutes), groups of up to 3 students
Weighting: 100 %
Final assessment: Yes
Group work: Yes
Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Presentation (Resit)
Description: Group presentation (30 minutes), groups of 1 to 3 students
Weighting: 100 %
Final assessment: Yes
Group work: Yes
Learning outcomes tested: MO1, MO2, MO3, MO4, MO5

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security [Frenchay] MSc 2023-24

Cyber Security [Frenchay] MSc 2023-24

Cyber Security [GCET] MSc 2023-24