



Module Specification

Security Management in Practice

Version: 2025-26, v5.0, Approved

Contents

Module Specification	1
Part 1: Information	2
Part 2: Description	2
Part 3: Teaching and learning methods	3
Part 4: Assessment.....	4
Part 5: Contributes towards	5

Part 1: Information

Module title: Security Management in Practice

Module code: UFCFRB-15-3

Level: Level 6

For implementation from: 2025-26

UWE credit rating: 15

ECTS credit rating: 7.5

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

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: This module will provide students with an understanding of Information Security Management Systems (ISMS), to assess information risk in the context of business operations.

Features: Not applicable

Educational aims: Through case studies and real-world news events, students will explore cyber security issues from the perspective of risk, and how companies can

manage risk that is associated with information assets. Students will work to develop their own ISMS plans for a chosen organisation, and will learn to developing their critical thinking skills through justification of proposed actions to mitigate risk.

Outline syllabus: Policies for managing security, policy languages and models
Information Security Management Standards. Codes of Practice. Legislation.

Security analysis; assumptions made, social basis and threat assumptions.

Planning for an ISMS

Information security risk assessment: risk analysis methods, risk treatment

Planning and managing a disaster recovery operation. Business Continuity Planning

Part 3: Teaching and learning methods

Teaching and learning methods: A series of seminars at the start of the module will cover background knowledge. The seminars will be predominantly tutor-led. Students are expected to prepare for the seminars by reading from the module text and from research papers as directed. They are also expected to identify their own information (see below). The seminars will then explore the issues raised by the reading, usually based on worksheets and often in the context of a case study.

The coursework will require the students will perform a security analysis of an organisation's information systems, propose a security policy and make recommendations about the implementation of that policy. This work will be based on the analysis of real organisation and may be conducted with an external organisation if it can be arranged.

Independent learning includes hours engaged with essential reading, case study preparation, assignment preparation and completion etc.

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

MO1 Demonstrate understanding of the significance of ISO and other standards in the specification of an Information Security Management System (ISMS)

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

MO3 Evaluate the significance of security laws and regulations

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 114 hours

Face-to-face learning = 36 hours

Reading list: The reading list for this module can be accessed at [readinglists.uwe.ac.uk](https://uwe.rl.talis.com/modules/ufcfrb-15-3.html) via the following link <https://uwe.rl.talis.com/modules/ufcfrb-15-3.html>

Part 4: Assessment

Assessment strategy: The module is assessed by a group presentation. Students will be required to work in allocated groups, and prepare a presentation focusing on a business/organisation of their choice.

Resit will be the same as sit - group presentation.

Assessment tasks:

Presentation (First Sit)

Description: Group presentation (15 mins)

Weighting: 100 %

Final assessment: Yes

Group work: Yes

Learning outcomes tested: MO1, MO2, MO3

Presentation (Resit)

Description: Group presentation (15 mins)

Weighting: 100 %

Final assessment: Yes

Group work: Yes

Learning outcomes tested: MO1, MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2023-24

Cyber Security and Digital Forensics [NepalBrit] BSc (Hons) 2023-24

Business Computing {Foundation} [Sep][SW][Frenchay][5yrs] BSc (Hons) 2021-22

Business Computing [Frenchay] BSc (Hons) 2023-24

Business Computing {Foundation} [Feb][SW][GCET][5yrs] BSc (Hons) 2021-22

Business Computing {Foundation} [Oct][SW][GCET][5yrs] BSc (Hons) 2021-22

Cyber Security and Digital Forensics {Foundation} [Sep][SW][Frenchay][5yrs] BSc (Hons) 2021-22

Business Computing {Foundation} [GCET] BSc (Hons) 2022-23

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2022-23

Information Technology {Top-Up} [Gloscoll] BSc (Hons) 2025-26

Cyber Security and Digital Forensics {Foundation} [Sep][SW][Frenchay][5yrs] BSc (Hons) 2021-22

Cyber Security and Digital Forensics {Foundation} [Frenchay] BSc (Hons) 2022-23

Cyber Security and Digital Forensics [Frenchay] BSc (Hons) 2022-23

Computer Security and Forensics {Foundation} [GCET] BSc (Hons) 2022-23

Business Computing {Foundation} [Frenchay] BSc (Hons) 2022-23

Business Computing {Foundation} [GCET] BSc (Hons) 2022-23

Business Computing [Frenchay] BSc (Hons) 2022-23

Information Technology {Dual}[Taylors] BSc (Hons) 2023-24

Information Technology {Top-Up} [Frenchay] BSc (Hons) 2024-25

Information Technology {Dual}[Taylors] BSc (Hons) 2023-24

Information Technology {Top-Up} [INTUNI] BSc (Hons) 2024-25

Information Technology {Top-Up} [Frenchay] BSc (Hons) 2025-26