Module Specification

Information management and security

Version: 2025-26, v2.0, 04 Mar 2025

Contents

Part 1: Information

Module title: Information management and security

Module code: UFCFKU-30-2

Level: Level 5

For implementation from: 2025-26

UWE credit rating: 30

ECTS credit rating: 15

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: Information security is concerned with protecting an organisations' electronic or physical data. It should protect the confidentiality, availability and integrity of data.

This module is concerned with the way in which electronic data is handled within the organisation, how it is made available, manipulated and analysed. It then examines

how management systems are employed to minimise risk without impacting business productivity.

Features: Not applicable

Educational aims: This module contributes cyber management knowledge and understanding.

Outline syllabus: You will cover

information management concepts, e.g.:

information storage and retrieval;

information capture and representation;

searching, retrieving, linking, navigating

database concepts, e.g.:
components of database systems;
design of core DBMS functions (e.g. query mechanisms, access methods);
database architecture and query language

big data, e.g.: benefits and limitations, components and architectures employed in systems for big data (e.g. Hadoop cluster, JSON) ,
tools and techniques for analysing large heterogeneous data sets, including statistics

graph theory

key concepts and benefits of information security management system

internationally recognised standards – e.g., ISO27001, or similar

governance, organisational structure, roles, policies, standards and guidelines for cyber and information security

how an organisation's security policies, standards and governance are supported by provisioning and access rights – e.g., how identity and access management are implemented and maintained for a database application or physical access control system

how cyber security policies and procedures are used in different organisational environments and affect individuals and organisations

the roles of experts in the cyber security industry, how they are recognised, and the work they do.

how to use organisations such as a CERT, OSINT provider, incident response provider

Part 3: Teaching and learning methods

Teaching and learning methods: The initial part of the module teaches students the basic concepts of information management and how to use database management systems.

The latter part covers the standards, policies and procedures for information security. These will cover human behaviour as well as physical and electronic assets.

Lecture sessions cover the technical knowledge required. Designated practical work is included to ensure that apprentices have absorbed and understood the key principles involved.

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

MO1 Apply statistical techniques to large data sets. Identify vulnerabilities in big data architectures and deployment.

MO2 Select an appropriate management system and use it to develop an information security management plan.

MO3 Explain the key concepts of information management.

MO4 Design a relational database using best practice techniques

MO5 Create and use a database via a DBMS .

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 135 hours

Placement = 75 hours

Face-to-face learning = 90 hours

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/CD43F295-21E6-83F5-3D12-BB3533A50A76.html

Part 4: Assessment

Assessment strategy: This module is assessed by a a presentation and a portfolio.

A presentation (30 minutes) of an information security plan for the apprentice's organisation. It should cover:
Compliance with ISO27001
The organisation's security policies and procedures
The use of CERT and OSINT

This allows the students to contextualise their theoretical knowledge within the context of an organisation with which they are familiar and brings to life the challenges of auditing and managing information assets.

The portfolio allows the students to concentrate on an alternative aspect of security management, the management of data. In the first part of the portfolio, students will design, create and use a database through a DBMS and explain information

concepts . Having demonstrated their grasp of the technicalities of data management, in the second part of the portfolio of work, they will deal with the presentation and operational aspects of data management by extracting and presenting data (including graphs) from a large dataset. They will explain potential issues with the management of large datasets (approx. 3000 words or equivalent in total).

The resit assessment strategy is the same as the first sit.

Assessment tasks:

Portfolio (First Sit)
Description: Portfolio composed of elements that demonstrate the storage, management, presentation and operational aspects of data management (1500 words).
Weighting: 75 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO3, MO4, MO5

Presentation (First Sit)
Description: Presentation (20 mins presentation and 10 mins Q&A)
Weighting: 25 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2

Presentation (Resit)
Description: Presentation (20 mins presentation and 10 mins Q&A)
Weighting: 25 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2

Portfolio (Resit)
Description: Portfolio composed of elements that demonstrate the storage, management, presentation and operational aspects of data management (1500 words).
Weighting: 75 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO3, MO4, MO5

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security Technical Professional {Apprenticeship-GLOSCOLL} [GlosColl] BSc (Hons) 2024-25