Prifysgol Wrecsam
Wrexham University

Module specification

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking on the following link: Module directory

Module Code	COM476
Module Title	Information Security and Governance
Level	4
Credit value	20
Faculty	FACE
HECoS Code	100376
Cost Code	GACP

Programmes in which module to be offered

Programme title	Is the module core or option for this programme
BSc (Hons) Computer Science	Core
BSc (Hons) Computer Science with Industrial Placement	Core
BSc (Hons) Cyber Security	Core
BSc (Hons) Cyber Security with Industrial Placement	Core
BSc (Hons) Software Engineering	Core
BSc (Hons) Software Engineering with Industrial Placement	Core

Pre-requisites

N/A

Breakdown of module hours

Learning and teaching hours	36 hrs
Placement tutor support	0 hrs
Supervised learning e.g. practical classes, workshops	0 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total active learning and teaching hours	**36** hrs
Placement / work based learning	0 hrs
Guided independent study	164 hrs
Module duration (total hours)	**200** hrs

For office use only	
Initial approval date	08/11/2023

For office use only	
With effect from date	Sept 2024
Date and details of revision	
Version number	1

Module aims

This module aims to equip students with the knowledge, skills, and professional mindset required to tackle complex information security challenges, ensure effective governance, and contribute to the protection of information assets in various organizational contexts. Students will gain an appreciation of regulation and how this can be implemented through policies and procedures in a digital world

Module Learning Outcomes - at the end of this module, students will be able to:

1	Research and appraise professional skills related to computing and develop a professional and ethical approach to practice.
2	Apply appropriate compliance laws, regulation and standards that affect businesses today.
3	Apply information security standards to real-world applications in both the private and public sector.
4	Identify global laws and regulations for information security.
5	Interpret the various industrial certifications relevant in the computing industry.

Assessment

Indicative Assessment Tasks:

This section outlines the type of assessment task the student will be expected to complete as part of the module. More details will be made available in the relevant academic year module handbook.

The learning outcomes of this module will be assessed in two components: a written assessment and an in-class assessment. The written assessment that be approximately 1800 words will demonstrate a student's understanding of risk assessment and mitigation in the context of information security and governance, while the in-class assessment will be an online quiz looking at various the laws and regulations which will take around 90mins.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	1,2,3	Written Assignment	50%
2	4,5	In-class test	50%

Derogations

None

Learning and Teaching Strategies

In line with the Active Learning Framework, this module will be blended digitally with both a VLE and online community. Content will be available synchronously and asynchronously and will include the key concepts, ideas, theories, and examples. Discussion boards and other online learning activities will allow for the further exploration of the topics to give students the opportunity to investigate, discuss and acquire further subject specific knowledge and understanding and how this applies to the real-world environment.

Indicative Syllabus Outline

Yearly content will be updated to represent the most appropriate content for current industry technologies, but a list of indicative topics could include:

- Risk management
- Security operations and incident response
- Identity and access management
- Legal and Regulatory Compliance
- Security governance and strategy
- Emerging technologies and trends
- Professionalism and social responsibility
    - Ethical
    - Social
    - Sustainability
    - Political aspects
    - Usability
    - Security
    - Accountability.

Indicative Bibliography:

Please note the essential reads and other indicative reading are subject to annual review and update. Please *ensure correct referencing format is being followed as per University Harvard Referencing Guidance.*

Essential Reads

N/A

Other indicative reading

A. Taylor, D. Alexander, A. Finch and D. Sutton, *Information Security Management Principles,* 3rd ed., BCS, The Chartered Institute of IT, 2020.

R. Anderson, *Security Engineering,* 3rd ed., Wiley, 2020.

R. E. Smith, *Elementary Information Security*, 3rd ed., Jones and Bartlett.

Financial Conduct Authority, 2023. [Online]. Available: https://www.fca.org.uk/ .

Information Commissioner's Office, 2023. [Online]. Available: http://www.ico.org.uk/.

Ofcom, 2023. [Online]. Available: https://www.ofcom.org.uk/home.