Information Security Management

Module Information

2022.01, Approved

Summary Information

Module Code	7539CYQR
Formal Module Title	Information Security Management
Owning School	Computer Science and Mathematics
Career	Postgraduate Taught
Credits	20
Academic level	FHEQ Level 7
Grading Schema	50

Teaching Responsibility

LJMU Schools involved in Delivery
LJMU Partner Taught

Partner Teaching Institution

Institution Name
Oryx Universal College WLL

Learning Methods

Learning Method Type	Hours
Lecture	11
Seminar	22

Module Offering(s)

Display Name	Location	Start Month	Duration Number Duration Unit
APR-PAR	PAR	April	12 Weeks
JAN-PAR	PAR	January	12 Weeks

SEP-PAR	PAR	September	12 Weeks

Aims and Outcomes

Aims	To develop a deep appreciation of information security problemsTo develop skills relating to security risk assessment and control analysisTo develop an appreciation of the complexity of using standards such as ISO-27001To gain experience in engaging in debates around legal, ethical and professional issues relating to information security.

After completing the module the student should be able to:

Learning Outcomes

Code	Number	Description
MLO1	1	Critically evaluate a complex information system in terms of its security
MLO2	2	Apply security risk assessment methods to a complex information system.
MLO3	3	Show critical awareness of the significant challenges involved in managing information security processes using standards
MLO4	4	Appreciate complex legal and ethical situations relating to information system security

Module Content

Outline Syllabus	Concepts in information management: information, management, processes, human factors, standards, compliance.Security fundamentals: threats, vulnerabilities, attacks, risk, models for security, defence, controls, and constraints (e.g. economic/business) on managing security.Understanding Information Security Management: risk assessment, policy, controls, personnel, education, monitoring and review, compliance, assurance.Risk Management and Risk AssessmentStandards for ISM: ISO/27001 and PCI-DSSDigital forensics, incident response, business continuity.Legal constraints: data protection and privacy, intellectual property, computer misuse, surveillance, fraud.Professional issues: ethics, privacy, professional bodies, certification.
Module Overview	
Additional Information	The term Information Security Management generally refers to the wide range of ongoing processes that information security practitioners engage in, although typically excludes development of solutions through software development. The module will develop analysis skills in understanding security threats, vulnerabilities, attacks and risks, as well as focussing is on management standards (such as PCI-DSS and ISO27001) and information governance, compliance, ethical and legal aspects of being an information security professional.

Assessments

Assignment Category	Assessment Name	Weight	Exam/Test Length (hours)	Module Learning Outcome Mapping
Report	Risk Assessment	40	0	MLO1, MLO2
Exam	Examination	60	2	MLO3, MLO4

Module Contacts

Module Leader

Contact Name	Applies to all offerings	Offerings
Bob Askwith	Yes	N/A

Partner Module Team

Contact Name	Applies to all offerings	Offerings