Liverpool John Moores University

Title:	INFORMATION SECURITY MANAGEMENT
Status:	Definitive
Code:	**7139COMP** (122211)
Version Start Date:	01-08-2021
Owning School/Faculty:	Computer Science and Mathematics
Teaching School/Faculty:	Computer Science and Mathematics

Team	Leader
Robert Askwith	Y
Aine MacDermott	

Academic Level:	FHEQ7	**Credit Value:**	20	**Total Delivered Hours:**	35
Total Learning Hours:	200	**Private Study:**	165		

Delivery Options
Course typically offered: Semester 1

Component	Contact Hours
Lecture	11
Seminar	22

Grading Basis: 50 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Report on security analysis and risk assessment of an information system	40	
Exam	AS2	Examination	60	2

Aims

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

Learning Outcomes

After completing the module the student should be able to:

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

Learning Outcomes of Assessments

The assessment item list is assessed via the learning outcomes listed:

Risk Assessment	1	2
Examination	3	4

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 Assessment

Standards for ISM: ISO/27001 and PCI-DSS

Digital forensics, incident response, business continuity.

Legal constraints: data protection and privacy, intellectual property, computer misuse, surveillance, fraud.

Professional issues: ethics, privacy, professional bodies, certification.

Learning Activities

Students will participate in lectures, tutorials/seminar sessions, including practicing risk assessment by using a software tool to produce a risk report. These sessions are to help students get a better understanding of the application of theory, in order to improve their learning before the exam.

Notes

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.