Liverpool John Moores University

Title:	Information Security Management
Status:	Definitive
Code:	**5219COMP** (127995)
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
Syed Naqvi	

Academic Level:	FHEQ5	**Credit Value:**	20	**Total Delivered Hours:**	46
Total Learning Hours:	200	**Private Study:**	154		

Delivery Options
Course typically offered: Semester 1

Component	Contact Hours
Lecture	22
Tutorial	22

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Report	AS1	Security Risk Analysis	40	
Exam	AS2	Examination	60	2

Aims

To provide a detailed understanding of the main concepts of information security management.
To develop an appreciation of the process of information security management, including risk analysis, control analysis and post-event security.
To develop an awareness of the standards relating to information security management within enterprise environments, including legal and compliance issues.

Learning Outcomes

After completing the module the student should be able to:

1	Analyse security risks associated with a computer system using a standard methodology.
2	Interpret legal, governance and compliance issues for information assurance.
3	Identify success factors in information security management.

Learning Outcomes of Assessments

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

Security Risk Analysis	1	
Examination	2	3

Outline Syllabus

Concepts in Information Security; threats, vulnerabilities, attacks, models for discussing security, situational awareness, economic and business constraints, technology controls, human factors, ethics, 'cyber'.
Risk Assessment; understanding risk factors, methods for risk assessment, contemporary standards such as ISO, FAIR, and NIST.
Information Security Management: governance and compliance, 'Quality' and the need for audit, standards including PCI-DSS and ISO 27000.
Law: the UK legal system, cyber-crime and related laws including CMA, DPA, GDPR, RIPA. Security 'conflicts' relating to privacy, surveillance, control and free-speech.
Post-event Security: attacks, incident response, disaster recovery, forensics and the involvement of law enforcement.

Learning Activities

Students will participate in lectures and tutorial sessions.

Notes

Information Security Management generally refers to the wide range of activities that information security practitioners engage in, although typically excludes the actual development of secure solutions through software development. In this module the focus is on the security risk analysis, management and information governance and compliance aspects of being an information security practitioner.