

Liverpool John Moores University

Title: COMPUTER SECURITY
Status: Definitive
Code: **6052BUSIS** (108250)
Version Start Date: 01-08-2011

Owning School/Faculty: Liverpool Business School
Teaching School/Faculty: Liverpool Business School

Team	Leader
Philip Kelly	Y

Academic Level: FHEQ6
Credit Value: 12.00
Total Delivered Hours: 27.00
Total Learning Hours: 120
Private Study: 93

Delivery Options

Course typically offered: Semester 2

Component	Contact Hours
Lecture	12.000
Tutorial	12.000

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Essay	AS1	Students will submit an assignment consisting of a 3000 word academic essay during studies.	50.0	
Exam	AS2	Students will sit a 3 hr examination.	50.0	3.00

Aims

To provide a clear, well-structured and interesting treatment of why and how organisations are vulnerable to loss, destruction, damage, unauthorised access and misuse of business information (BI). The module will provide a logical path through the understanding of BI threats, attacks and consequences, controls and countermeasures to the establishment of a proactive and professional BI culture.

Formal, manual and computer-based, and informal information systems will be considered as will the common business information technologies.

Learning Outcomes

After completing the module the student should be able to:

- 1 Understand IS risk in the context of the organization, Business Information Systems, Risk Management and security.
- 2 Describe common business information (BI) and information system (IS) threats, vulnerabilities and risks and controls and countermeasures.
- 3 Explain the Risk Management (RMP) and Business Continuity Management (BCM) processes and how they are used to make BI/IS risk decisions.
- 4 Identify common sources of IS security best practice.
- 5 Explain why software and databases are vulnerable to attack; identifying specific threats and controls to protect such IS system resources.
- 6 Describe the security technologies used to protect the contemporary digital organization.
- 7 Discuss a range of methods used to improve user awareness of IS security.

Learning Outcomes of Assessments

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

CW	1	2	3	4	5	6	7
EXAM	1	2	3	4	5	6	7

Outline Syllabus

The Organizational Context
Business Information Systems
Risk Management
Security - an Introduction
Business Information Risk - Threats, Hazards & Vulnerabilities
Business Information Risk - Controls and Countermeasures
Business Information Risk Management
Business Information Risk - codes, standards & legislation
Securing Data, Databases and Software
Securing the Digital Organization
Security Organization
Security Conscience

Learning Activities

Lectures and tutorials.

References

Course Material	Book
Author	Kelly, P P
Publishing Year	0
Title	Information Systems Risk
Subtitle	
Edition	
Publisher	Wittherbys
ISBN	

Notes

Looks at the variuors aspects of Computer Security.