MODULE SPECIFICATION PROFORMA

Module Code:	COM744

Module Title:	Security and Risk Management

Level:	7	**Credit Value:**	20

Cost Centre(s):	GACP	JACS3 **code**: HECoS code:	I250 100756

Faculty:	Arts, Science and Technology	**Module Leader:**	Denise Oram

Scheduled learning and teaching hours	21 hrs
Guided independent study	179 hrs
Placement	0 hrs
Module duration (total hours)	200 hrs

Programme(s) in which to be offered (not including exit awards)	Core	Option
MSc Cyber Security	✓	☐
MComp Computer Science	✓	☐
MSc Computing	✓	
MSc Computer Science	✓	

Pre-requisites
None

Office use only

Initial approval: 28/11/2018 Version no:1

With effect from: 01/09/2019

Date and details of revision: 17/03/20, added to MSc Computing and MSc Computer Science Version no:2

Module Aims
This module is aimed at providing students with the understanding of security risks associated with information assets and the security programs designed to protect them from security threats. This module will focus on the identification of security risks, the application of risk control and risk management measures, the appreciation of security technology, and critical understanding of security policies, standards and practices. The legal, ethical, and professional issues in security management are also covered in this module.

Intended Learning Outcomes

Key skills for employability

KS1	Written, oral and media communication skills
KS2	Leadership, team working and networking skills
KS3	Opportunity, creativity and problem solving skills
KS4	Information technology skills and digital literacy
KS5	Information management skills
KS6	Research skills
KS7	Intercultural and sustainability skills
KS8	Career management skills
KS9	Learning to learn (managing personal and professional development, self-management)
KS10	Numeracy

At the end of this module, students will be able to		Key Skills	
1	Understand the issues with information security and security risks.	KS1	
		KS5	
		KS6	
2	Identify the security risks and risk and security control strategies in a particular context.	KS1	KS6
		KS3	
		KS5	
3	Evaluate various security technologies.	KS1	
		KS5	
		KS6	
4	Understand and apply business continuity planning for a given scenario.	KS1	
		KS5	
		KS6	
5	Understand and apply security policy, standard, and practices.	KS1	KS6
		KS3	
		KS5	
6	Discuss issues related to legal, ethical, and professional issues in security management.	KS1	
		KS5	
		KS6	

Transferable skills and other attributes

Derogations

None

Assessment:

Indicative Assessment Tasks:

The learning outcomes of this module will be assessed in two components: an assignment and an in-class test. The assignment is a case study report (4000 words) – which will involve applying the learning outcomes to a given scenario. Students will have opportunities of informative feedback in workshops throughout the semester and in tutorials where appropriate.

Formative assessment and feedback opportunities will be provided to develop student understanding of the subject.
The class test (1.5 hours) is used to assess students' deeper understanding of the learning outcomes.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)	Duration (if exam)	Word count (or equivalent if appropriate)
1	1-6	Case Study	70		4000
2	1,2,5,6	In-class test	30	1.5 hours	

Learning and Teaching Strategies:

Students will develop theoretical understanding and practical skills based on weekly lectures, tutorials and supervised workshops. The workshops, in particular, are provided to support students in gaining practical experience in security management.
Appropriate blended learning approaches and technologies, will be used to facilitate and support student learning and to:
• deliver content;
• encourage active learning;
• provide formative and summative assessments, and prompt feedback;
• enhance student engagement and learning experience.

Students will be expected and encouraged to produce reflective commentaries on the learning activities and tasks that they carry out to complete their work.

Syllabus outline:

• Introduction and background to technology, crime and security
• Information assets and the issues with information security
• Security measures designed to protect information assets
• Identification of security threats and the design of risk control measures
• Security risk assessment and implementation of risk control strategies

• Information security standards and policies, for example; BS 7799 and BS ISO/IEC 17799:2000, ISO 27001
• Protection mechanisms
• Legal, ethical, and professional issues
• Information security maintenance
Business Continuity Planning

Indicative Bibliography:

Essential reading

L.M. Zeichner, L.M. (2014). Cybersecurity foundations: An interdisciplinary introduction, Zeichner Risk Analytics.

Calder, A and Watkins, S. (2015). IT governance: An international guide to data security and iso27001/iso27002, Kogan Page.

Calder, A. (2016) Nine steps to success: An iso 27001 implementation overview, IT Governance Limited.

Mooney, T. (2015). Information security a practical guide: Bridging the gap between it and management, IT Governance Publishing.

Nayak, U. and Rao, U.H. (2014). The InfoSec handbook: An introduction to information security,Apress.

British Standards Institute Staff and Brewer, D. (2013). An introduction to iso/iec 27001:2013, BSI Standards.

Taylor, A., Alexander, D., Finch, A., and Sutton, D. (2013). Information security management principles, BCS Learning & Development Limited.

Other indicative reading

Watkins, S. (2013). An introduction to information security and iso27001:2013: A pocket guide, IT Governance.

Solomon, M.G. and Chapple, M. (2009). Information security illuminated, Jones & Bartlett Learning.

Mitnick, K.D. and Simon, W.L. (2009). The art of intrusion: The real stories behind the exploits of hackers, intruders and deceivers, Wiley.

Mitnick, K.D., Simon, W.L. and Wozniak, S. (2011). The art of deception: Controlling the human element of security, Wiley, 2011.