MODULE SPECIFICATION

When printed this becomes an uncontrolled document. Please access the Module Directory for the most up to date version by clicking here.

Refer to guidance notes for completion of each section of the specification.

Module Code:	CONL721

Module Title:	Security and Risk Management in a Digital Environment

Level:	7	**Credit Value:**	15

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

Faculty	FAST	**Module Leader:**	Denise Oram

Scheduled learning and teaching hours	15 hrs
Placement tutor support	0 hrs
Supervised learning eg practical classes, workshops	0 hrs
Project supervision (level 6 projects and dissertation modules only)	0 hrs
Total contact hours	15 hrs
Placement / work based learning	0 hrs
Guided independent study	135 hrs
Module duration (total hours)	150 hrs

Programme(s) in which to be offered (not including exit awards)	Core	Option
MBA Cyber Security	✓	□
MSc Computer Science (online)	✓	□
MSc Computer Science with Big Data Analytics	✓	□
MSc Computer Science with Cyber Security	✓	□
MSc Computer Science with Networking	✓	□
MSc Computer Science with Software Engineering	✓	□

Pre-requisites
None

MODULE SPECIFICATION

Office use only	
Initial approval: 04/06/2020	Version no: 1
With effect from: 01/09/2020	
Date and details of revision: Oct 2020: APSC approved assessment change	Version no:2

Module Aims
The module will focus on the identification and exploration of security risks, the application of risk control and risk management measures and regulation. Students will gain appreciation of security technology and critical understanding of security policies, standards and practices as well as the legal, ethical, and professional issues in security management.

Module Learning Outcomes - at the end of this module, students will be able to	
1	Make informed judgements by critically evaluating the issues with information security and security risks.
2	Identify and explore issues related to legal, ethical and professional issues in security management.
3	Critically evaluate various security technologies.
4	Evaluate and discuss risk control and risk management measures.

Employability Skills **The Wrexham Glyndŵr Graduate**	**I = included in module content** **A = included in module assessment** **N/A = not applicable**
CORE ATTRIBUTES	
Engaged	I A
Creative	A
Enterprising	N/A
Ethical	I A
KEY ATTITUDES	
Commitment	I A
Curiosity	A
Resilient	I A
Confidence	A
Adaptability	I A
PRACTICAL SKILLSETS	
Digital fluency	I A
Organisation	A
Leadership and team working	I
Critical thinking	I A
Emotional intelligence	I A
Communication	A

Derogations

NONE

Assessment:

Indicative Assessment Tasks:

Assessment 1 will be a 1,200-word report discussing and critically evaluating security risks and various security technologies, and will be submitted during Week 4.

Assessment 2 will be a 1,800-word essay during Week 8 evaluating the legal, professional and ethical issues encountered in security management as well as the security technologies that may be implemented to mitigate these risks.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)
1	3,4	Report	40%
2	1,2	Essay	60%

Learning and Teaching Strategies:

The overall learning and teaching strategy is one of guided independent study requiring ongoing student engagement. Online material will provide the foundation of the learning resources, requiring the students to login and engage on a regular basis throughout the eight week period of the module. There will be a mix of suggested readings, discussions and interactive content containing embedded digital media and self-checks for students to complete as they work through the material and undertake the assessment tasks. The use of a range digital tools via the virtual learning environment together with additional sources of reading will also be utilised to accommodate learning styles. There is access to a helpline for additional support and chat facilities through Canvas for messaging and responding.

Syllabus outline:

1. Introduction and background to Security and Risk Management
2. Asset Security
3. Security Engineering and communication
4. Identification of security threats and access management
5. Security risk assessment, operations and implementation of risk control strategies
6. Legal, ethical, and professional issues
7. Information security maintenance

Indicative Bibliography:

Essential reading

Darril Gibson, Andy Igonor, (2020); *Managing Risk in Information Systems.* 3rd edition. Jones & Bartlett Learning. ISBN: 9781284183719.

Other indicative reading

Schmidt, W. (2019) CISSP: *A Comprehensive Beginners Guide on the Information systems Security.*

Calder, A and Watkins, S. (2015) *IT governance: An international guide to data security and ISO27001/ISO27002*. Kogan Page.

Kirwan, G and Power, A. (2013) *Cybercrime; the Psychology of Online Offenders.* Cambridge University Press.

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