



Title:	Security Management and Law APPROVED
Long Title:	Security Management and Law
Module Code:	COMP9082
Duration:	1 Semester
Credits:	10
NFQ Level:	Expert
Field of Study:	Computer Science
Valid From:	Semester 1 - 2020/21 (September 2020)
Module Delivered in	2 programme(s)
Module Coordinator:	Sean McSweeney
Module Author:	NOREEN GUBBINS
Module Description:	This module examines national and EU laws, regulations and acts relevant to the field of cybersecurity and their impact in strengthening Ireland and the EU ability in tackling cybersecurity threats, attacks and cybercrime. In addition, this module will examine cybersecurity management frameworks and practices with the aim of improving an organisation's security posture and enhance resilience's against cyberattacks.
Learning Outcomes	
<i>On successful completion of this module the learner will be able to:</i>	
LO1	Critically evaluate the laws and the relationship between laws with ethics in the domain of Information & Communication Technologies (ICT).
LO2	Evaluate national and international laws pertaining to cybercrime acts and their impact to individuals and organisations.
LO3	Assess the main issues relating to intellectual property and the intangible rights of ownership as it relates to software.
LO4	Analyse the main EU Data Protection Laws in relation to protecting EU citizens data and their respective security.
LO5	Critically evaluate security models and frameworks in their ability to serve as a roadmap to organise cybersecurity management activities in an organisation.
LO6	Evaluate security management practices in managing an organisations information assets in areas such as privacy, confidentiality, integrity and accountability.
LO7	Utilise project planning techniques and examine leadership styles within security management.
Pre-requisite learning	
Module Recommendations <i>This is prior learning (or a practical skill) that is strongly recommended before enrolment in this module. You may enrol in this module if you have not acquired the recommended learning but you will have considerable difficulty in passing (i.e. achieving the learning outcomes of) the module. While the prior learning is expressed as named CIT module(s) it also allows for learning (in another module or modules) which is equivalent to the learning specified in the named module(s).</i>	
Incompatible Modules <i>These are modules which have learning outcomes that are too similar to the learning outcomes of this module. You may not earn additional credit for the same learning and therefore you may not enrol in this module if you have successfully completed any modules in the incompatible list.</i>	
No incompatible modules listed	
Co-requisite Modules	
No Co-requisite modules listed	

Requirements

This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed. You may not enrol on this module if you have not acquired the learning specified in this section.

No requirements listed

Module Content & Assessment

Indicative Content

Law, Ethics & ICT

The meaning of 'Ethics'. The key sources of law relating to computing. European Union Law, Legislation and Judicial Precedent. The impact of the Constitution. The relationship between Law and Morality. Ethical issues in computing. GDPR, NIS, CFA Act, CSA Act, ECPA, HIPAA, GLB Act, SOX, DMCA, CCPA

Computer Crime & Fraud

Most common cybercrime acts - fraud, phishing scams, fraudulent sales, financial cybercrime, hacking, identity theft, scamming, viruses, ransomware, DDoS attacks, online harassment, cyberstalking etc. Characteristics of victims. Estimating the cost of cybercrime in Ireland and EU. The development of offences related to computing in Irish and International Law. Comparison with other jurisdictions. The implementation of computer crime legislation. EU Fraud and corruption legislation and strategy. Criminal Justice Act.

Intellectual Property and Computer Software

General rules of copyright. Application of Copyright to software. Remedies and enforcement. Evaluation of the current approach and comparison with other jurisdictions. patents, Trademarks, Service Marks.

EU Data Protection

Directive on Privacy and Electronic Communications (ePrivacy Directive) – EU Telecoms data protection frameworks. Personal Data Breaches – how to deal with them. Irish Data Protection Acts 1988 -2018. General Data Protection Regulation (GDPR) - Data Processing – situations where it is allowed, agreeing to and withdrawing consent, GDPR and children, accessing, correcting and deleting your personal data. Complaints. Cookies. Data Protection Authorities. Compensation. Data Protection Act 2018.

Data Commissioner

European Data Protection Board. Data Protection Commission. Data Protection Officer. Independent Supervisory Authorities. DPC and role in regulating technology firms. High profile cases in data privacy in Ireland i.e. Public Service Identity Card etc. Data breaches notifications.

Security Leadership

Leadership Styles (e.g. Autocratic, Democratic, Delegative), Motivational Factors, McGregor Theory, Visionaries, Team dynamics, Personality Types, Performance Management, Change Management

Cybersecurity Management Models and Frameworks

ISO/IEC 27000 series of standards, NIST Cybersecurity Management Framework, NIST Framework for Improving Critical Infrastructure Security. CIS Critical Security Controls. PCI DSS. Operational Technology Cybersecurity Framework. IEC 62443. Security Architecture models. Access Control models. Academic Access control models - Bell LaPadula confidentiality model, Biba and Clark-Wilson integrity model.

Security Programme Development and Management

Security Programme Management - management of resources, procedures, performance. Security Programme Operations, Project management tools and techniques. Operational responsibilities and role delineation in security including legal considerations e.g. CISO, Security Manager, Security Architect.

Security Management Practices

Security Policies. Information Security Roles and Titles. Data protection and access. Information Security Professional Credentials. Trends in Certification and Accreditation. Employment Policies and Practices. Protection Mechanisms. Performance Measurement in Security Management. Security Awareness Training.

Cloud Security Management

Architecture of cloud services, overview of common cloud reference architectures, cloud infrastructures, partnerships and service management. The role & responsibilities of the Cloud Service Provider.

Assessment Breakdown

Assessment Breakdown	%
Course Work	100.00%

Course Work

Assessment Type	Assessment Description	Outcome addressed	% of total	Assessment Date
Essay	An essay critically analysing security models and frameworks.	1,5	20.0	Week 4
Written Report	A critical report on a legal or ethical issue from the module.	1,2,3,4	40.0	Week 10
Written Report	Project plan on implementing security management.	5,6,7	40.0	Sem End

No End of Module Formal Examination

Reassessment Requirement
Coursework Only <i>This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.</i>

The institute reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time				
<i>Workload Type</i>	<i>Workload Description</i>	<i>Hours</i>	<i>Frequency</i>	<i>Average Weekly Learner Workload</i>
Lecture	Lecture delivering theory underpinning learning outcomes	4.0	Every Week	4.00
Tutorial	Tutorial discussing topics in Security Management and Law	2.0	Every Week	2.00
Independent Learning	Independent Study.	8.0	Every Week	8.00
Total Hours				14.00
Total Weekly Learner Workload				14.00
Total Weekly Contact Hours				6.00

Workload: Part Time				
<i>Workload Type</i>	<i>Workload Description</i>	<i>Hours</i>	<i>Frequency</i>	<i>Average Weekly Learner Workload</i>
Tutorial	Lecture delivering theory underpinning learning outcomes	4.0	Every Week	4.00
Tutorial	Tutorial discussing topics in Security Management and Law	2.0	Every Week	2.00
Independent Learning	Independent Study.	8.0	Every Week	8.00
Total Hours				14.00
Total Weekly Learner Workload				14.00
Total Weekly Contact Hours				6.00

Module Resources

Recommended Book Resources

- Michael Whitman 2018, *Management of Information Security*, 6th ed. Ed., CENGAGE Learning Custom Publishing [ISBN: 9781337405713]

Supplementary Book Resources

- Raj Samani, Brian Honan, Jim Reavis 2014, *CSA Guide to Cloud Computing Implementing Cloud Privacy and Security*, Syngress [ISBN: 9780124201255]
- Denis Kelleher 2017, *Privacy and Data Protection Law in Ireland*, 2nd Ed., Bloomsbury Professional [ISBN: 9781780436159]
- Maeve McDonagh, Mícheál O'Dowd 2015, *CyberLaw in Ireland*, Kluwer Law International [ISBN: 9789041160058]

This module does not have any article/paper resources

Other Resources

- Website: *Safeguarding your information with ISO/IEC 27001* , National Standards Authority of Ireland
<https://www.nsai.ie/certification/management-systems/iso-iec-27001-information-security-management-system/>
- Website: *The Data Protection Commission Ireland*
<https://www.dataprotection.ie/>
- Website: *Denis Kelleher ICT Law in Ireland*
<http://www.ictlaw.com/>
- Website: *Digital Rights Ireland*
<https://www.digitalrights.ie/>

Module Delivered in

Programme Code	Programme	Semester	Delivery
CR_KCYMN_9	<u>Master of Science in Cybersecurity Management</u>	2	Mandatory
CR_KCYMT_9	<u>Postgraduate Diploma in Science in Cybersecurity Management</u>	2	Mandatory