Title	Cyber Security Standards and Risks
Long Title	Cyber Security Standards and Risks
Credits	**5**
NFQ Level	**Advanced**
Module Author	

Module Description:

In this module students will learn about risk management processes with a particular focus on how to manage the risk related to the use, processing, storage, and transmission of data. Laws, regulations, controls, compliance and violations as it pertains to personal information and data are also included as part of this module. This module was developed under the Cyber Skills HCI Pillar 3 Project. Please refer to consortium agreement for ownership

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1 Assess, manage and control the risk related associated to the use, processing, storage and transmission of data.

LO2 Identify key risk metrics with the aim of being able to mitigate against a particular risk scenario.

LO3 Appraise the laws, regulations, policies and ethics as they relate to cyber security and privacy

LO4 Evaluate key data security standards designed to protect personal information.

LO5 Assess and test an organizations procedures in the event of data compromise, and operational and financial impact of the violation/compromise.

Indicative Content

Risk Management

NIST Risk Management Framework. Risk assessment and risk cost. NIST Risk Management Process. Communicating and sharing risk assessment information. NIST – Cybersecurity for Business (align Business, IT and Cloud Security Standards). Cybersecurity Risk Management plan – identify company assets, cyber threats, impact and ranking of threats. Common Vulnerabilities and Exposures (CVE). Risk mitigation. The human element. Risk Management Process. Treating risk. Third party risk assessments.

Risk metric scenarios

Conducting a risk assessment. Risk management metrics for cybersecurity. Capturing risk and measuring risk correctly. Reducing, avoiding and transferring risk. Baselines,

benchmarks/CVSS, return on investment and cost-benefit analysis. Review of existing security. Risk mitigation strategies. Risk scenarios and responses. Pro-active and Reactive Threat Assessment (MITRE ATT&CK Framework, IBM X-Force).

Data Risk Management, Models & Controls

Opportunities and security challenges associated with data. Data risks - storage failures, data corruption, compliance, unused data. Backup and Disaster Recovery (BDR)

Solutions. Data security controls - Access privileges, application security, multi factor authentication. Penalties for non-compliance. Access Control models. Academic Access control models - Bell LaPadula confidentiality model, Biba and Clark-Wilson integrity model. Identifying and assessing gaps in security standards leading to security

breaches and compromised security controls. Bridging the gaps between Cybersecurity and Communication Standards.

Laws, Regulations & Standard

Ireland and EU: EU Cybersecurity Act, Personally Identifiable Information (PII), GDPR/Statutory Data Audit, NIS. Criminal Justice (Offences Relating to Information Systems) Act 2017. USA : CFA Act, CSA Act, ECPA, GLB Act, SOX, DMCA, CCPA. Personal Health Information (PHI) Health Insurance Portability and Accountability Act of 1996 (HIPAA). Payment Card Industry (PCI) Data Security Standard (DSS), ENISA Threat Landscape. The meaning of 'Ethics'. The relationship between Law and Morality.

Ethical issues in computing.

Standards, Compliance & Violation

Reporting standards. NIST. SSAE-16. AT-101. Federal Risk and Authorization Management Program (FedRAMP) compliance. ISO compliance. Regulatory Compliance. Reputational damage. Gambling Commission, Auditing. Skill in implementing and testing network infrastructure contingency and recovery plans.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Written Report	The learner will produce a written report to a professional standard applying cybersecurity governance frameworks to the mitigation of various cyber threats.	1,2	40	Week 6
Project	The focus of this project will be for the student to develop a cyber defense programme for an organisation in which a number of the current emerging technologies have been realized (e.g. cognitive EDR) which incorporates the impact this technology will have on current operations and security. The core focus of this project is quantifying the practical implication of these technologies and the financial and competitive advantage they may yield.	2,3,4,5	60	Sem End
No End of Module Formal Exam				

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework Only
This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2	Every Week	2.00
Lab	Lab to support learning outcomes.	1	Every Week	1.00
Independent & Directed Learning (Non-contact)	Independent learning.	4	Every Week	4.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		3.00

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2	Every Week	2.00
Lab	Lab to support learning outcomes.	1	Every Week	1.00
Independent & Directed Learning (Non-contact)	Independent Study.	4	Every Week	4.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		3.00

Recommended Book Resources

- Paul Hopkin 2018, Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management, 5th Ed. Ed., IRM Press [ISBN: 0749483075]