Title	Cybersecurity Risk Frameworks
Long Title	Cybersecurity Risk Frameworks
Credits	10
NFQ Level	Expert
Module Author	Gillian O'Carroll

Module Description:

In this module, Learners will examine the impact of risk management frameworks and develop a critical appreciation of risk management relating to the use, processing, storage and transmission of data. Learners will examine key laws, regulations, compliance and violations as pertaining to personal information and data. The module will enable learners to reflect on widely adopted cybersecurity risk management frameworks and critically appraise how these frameworks can be applied by organisations to minimise cybersecurity risk.

Learning Outcomes

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

LO1 Critically analyse the risks associated with the use, processing, storage and transmission of data.
LO2 Examine appropriate cybersecurity risk metrics to mitigate against various data risk scenarios.
LO3 Assess statutory laws, regulations, policies and ethics as they relate to cybersecurity and privacy.
LO4 Analyse key data security standards designed to protect personal information.
LO5 Evaluate effective organisational procedures in the event of data compromise, reflecting the operational and financial impacts of non-compliance.

Indicative Content

Risk Management

Risk Management Frameworks. The 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 Standards). Cybersecurity Risk Management Plan – identify company assets, cyber threats, impact and ranking of threats. Common Vulnerabilities and Exposures (CVEs). Risk mitigation. The human element. Treating risk. Third Party Risk Assessments.

Risk Metric Scenarios

Conducting a Risk Assessment. Risk management metrics for cybersecurity. Capturing 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. Proactive and Reactive Threat Assessment (MITRE 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 & Standards

Ireland and the EU: EU Cybersecurity Act, Personally Identifiable Information (PII), GDPR, NIS and NIS 2, Criminal Justice (Offences relating to Information Systems) Act 2017. ENISA Threat Landscape. USA: CFA Act, CSA Act, ECPA, GLB Act, DMCA, CCPA, Personal Health Information (PHI), Health Insurance Portability and Accountability Act 1996 (HIPPA), Payment Card Industry Data Security Standard (PCI DSS). Ethical issues in computing. The meaning of "Ethics". The relationship between law and morality.

Standards, Compliance and Violation

Reporting standards. NIST SSAE-16. AT-101. Federal Risk and Authorization Management Program (FedRAMP) compliance. ISO compliance. Regulatory compliance. 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 appraising the effectiveness of cybersecurity governance frameworks and judging their effectiveness in the mitigation of differing cybersecurity risks scenarios.	1,2	40.0	Week 6
Project	Learners must select the appropriate compliance, legal and governance mechanisms to implement and adhere to in a defined ambiguous cybersecurity scenario. Learners must defend their research, formulating a presentation capable of clearly supporting a summary of their findings to their peers and experts in the field.	3,4,5	60.0	Sem End

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 underpinning the learning outcomes.	2.0	Every Week	2.0
Lab	Lab to support content delivered.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	10.0	Every Week	10.00
		Total Hours		14.00
		Total Weekly Learner Workload		14.00
		Total Weekly Contact Hours		4.00

Workload – Part Time

Workload Type	Workload Description	Hours	Frequency	Average Weekly Leaner Workload
Lecture	Lecture underpinning the learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support content delivered.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	10.0	Every Week	10.00
		Total Hours		14.00
		Total Weekly Learner Workload		14.00
		Total Weekly Contact Hours		4.00

Recommended Book Resources

- **Cynthia Brumfield 2022, *Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework*, 1st Ed., Wiley [ISBN: 1119816289]**