Title	Information Security Architect
Long Title	Information Security Architect
Credits	5
NFQ Level	Expert
Module Author	Prof. Donna O'Shea

Module Description:

In this module the student will learn about information security and its importance in protecting the confidentiality, integrity and availability of systems and information. The student will develop the skills to discern between the different security needs of various stakeholders, evaluate the robustness of security designs and design security controls to protect information assets. This module was developed under the Cyber Skills HCI Pillar3 Project. Please refer to consortium agreement for ownership

Learning Outcomes

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

LO1	Discern between the different obligations and requirements that an organization need to consider to protect the confidentiality, integrity and availability of information.
LO2	Evaluate the engagement with information security at a governance level to achieve an organisation's sustainable protection of its information assets.
LO3	Assess and design security controls that should be considered as part of an overall Information Security Management (ISM) strategy.
LO4	Assess the role of Identity and Access Management (IAM) techniques as a method to control access to information assets.
LO1	Discern between the different obligations and requirements that an organization need to consider to protect the confidentiality, integrity and availability of information.

Indicative Content

Information Security Principles

What is information security? Information Security models - Confidentiality, Integrity, Availability (CIA) triad, Parkerian Hexad. Attacks on information – Interception, Interruption, Modification, Fabrication. Active and passive attacks in information security. Use cases on some of the more well-known attacks on information for example. Adobe, Facebook, Twitter, Playstation, Canva, Linkedin, Adult Friend Finder

Information Security Requirements

Obligations to consider at a business, regulatory, customer level. Business obligations - business continuity, end user security, risk management, security awareness, data protection, governance etc. Regulatory concerns - Personal Information Protection and Electronic Documents Act (PIPEDA), General Data Protection Regulation (GDPR) etc.

Information Security Governance (ISG)

Chief Information Officer (CIO) role and responsibilities. How to engage top level management in information security decisions. Culture and impact on ISG. Awareness programmes. Compliance & Assessment. ISG as a method of ensuring responsibility, accountability, and risk controls. Goals of ISG. Characteristic of good ISG. ISO27001, COBIT, ISO 38500, PRINCE2, PDCA Cycle, NIST, Enterprise Information Security Architecture (EISA).

Identity and Access Management (IAM)

What is IAM. Role of IAM as part of compliance. Authentication – Single Sign in, multifactor authentication, sessions, and token management. Authorization – roles, rules, attributes etc, User management and repositories i.e. directory services. Access management. Active Directory. Biometric authentication. Open standards. Challenges and risks.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	The learner is presented with a case study referring to a hypothetical or actual attack on an organisation's information system and is expected to consider the impact of the attack on the security requirements at a business, regulatory and customer level, in addition to how proper governance could have been used to protect the confidentiatly, integrity and availability of the system. The learner will document their work in a report produced to a professional standard.	1,2	40.0	Week 6
Project	The student will assess and design a range of security controls based on a presented case study. The learner will document their work in a report produced to a professional standard.	3,4	60.0	Sem End

No End of Module Formal Examination

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework

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	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.00
Lab	Interactive labs leveraging a sophisticated virtualised environment.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent Learning: preparing project deliverable, reading resource material and self-directed study.	3.0	Every Week	3.00
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.00
Lab	Interactive labs leveraging a sophisticated virtualised environment.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent Learning: preparing project deliverable, reading resource material and self-directed study.	3.0	Every Week	3.00
		Total Hours		7
		Total Weekly Learner Workload		7
		Total Weekly Contact Hours		4

Recommended Book Resources

- **Whitman, Michael E; Mattord, Herbert J 2018, *Management of information security*, 6th Ed., Cengage Learning [ISBN: 9781337405713]**