INFO08032
Cyber Security Architecture

Full Title	Cyber Security Architecture		
Status	Uploaded to Banner	**Start Term**	2020
NFQ Level	08	**ECTS Credits**	10
Module Code	INFO08032	**Duration**	Stage - (26 Weeks)
Grading Mode	Numeric	**Department**	Business, Humanities and Tech
Module Author	Mark Frain		

Module Description

This module practically demonstrates measures and controls that an organisation can deploy to improve threat mitigation capabilities and ensure compliance with the relevant frameworks. Measures such as security infrastructure, server and cloud services, secure networks and encryption ensure organisations comply with legal and ethical standards and mitigate against risk.

	Learning Outcomes ***On completion of this module the learner will/should be able to:***
1.	Explain the theory, concepts and methods that apply to Cyber Security Architecture.
2.	Identify relevant frameworks that apply to Cyber Security Architecture.
3.	Implement appropriate measures and controls that an organisation can deploy to improve threat mitigation capabilities and ensure compliance with relevant frameworks.
4.	Design, develop and apply techniques and technologies to ensure organisations comply with legal and ethical standards and mitigate against risk.
5.	Analyse and evaluate research topics in the area of Cyber Security Architecture individually or as part of a team.

Indicative Syllabus

Cyber Security Architecture (10%)

Key features of Cyber Security Architectures, Roles and Responsibilities, Policies, Standards and Guidelines.

Cyber Security Best Practice and Standards (20%)

Components of Cyber Security Frameworks, Monitor and Manage compliance with relevant standards — Information Security Standards, Cybersecurity Frameworks, COBIT 5 for Information Security, NIST, ISO 27001.

Cybersecurity Governance (10%)

Security Governance, Strategic Planning, Organizational Structure, Roles and Responsibilities, Integration with Enterprise Architecture, Policies and Guidance

Cyber Security Risk Management (20%)

Cyber Security Risk Management, Cyber Security Risk Assessment — ISO 27005, Cyber Security Risk Strategy, Cyber Security Architectural design, Cyber security Policies and Governance, Legal and Regulatory requirements.

Information Protection Concepts (20%)

Data Security protection, Processing of Data - obtaining, organising, retrieving, disclosing and erasing data. Confidentiality, integrity, and availability of information, Asset Management. Securing data by design and/or by default.

Identity and Access Management (IAM) (10%)

IAM Architecture. IAM Standards Federated Identities. Authentication and Authorisation. Investigate risk-based authentication strategies for cloud applications (e.g., authentication based on geo-location, device identifier etc.)

Security Incidence Response (10%)

Incident Response and Recovery Services, Endpoint Detection and Recovery. Disaster Recovery Planning, Backup and Recovery.

Teaching and Learning Strategy

This module can be delivered via the traditional face-to-face delivery methodology or via a blended format (employing both online and offline methodologies.) or via an online format.

Traditional face-to face delivery format.

The module can be delivered in the traditional delivery method using lectures/tutorials (2 hours per week) and lab practical's (2 hours per week).

Blended delivery format.

The module can be delivered in the blended delivery method using a mixture of online delivery (approx.. 75%) and face-to-face engagement (approx. 25%).

Weekly online delivery will consist of, but not exclusive to, live lectures and webinars, pre-recordings, synchronous and asynchronous discussion forums and open educational resources (OER's), exercises and reading, accounting for approx. 2 hours per week.

Online delivery format.

The module can be delivered in an asynchronous online method.

Information concerning the nature and timing of continuous assessment will be reviewed and agreed with learners and external examiners at the beginning of the academic year. Marking criteria, deadlines and expectations will also be provided to the learner in advance. Constructive feedback will be provided in a timely manner and in an appropriate format.

Independent Learning.

Allied to the Approved Programme Schedule hours students will be required to pursue Independent Learning as part of the module.

Assessment Strategy

This module will comprise 100% continuous assessment. The learner will be assessed on their practical ability and theoretical knowledge of Cyber Security Architectures.

Information concerning the nature and timing of continuous assessment will be reviewed and agreed with learners and external examiners at the beginning of the academic year. Marking criteria, deadlines and expectations will also be provided to the learner in advance. Constructive feedback will be provided in a timely manner and in an appropriate format.

Repeat Assessment Strategies

Repeat facilities will be accommodated in line with GMIT Code of Practice No. 3 Student Assessment: Marks & Standards procedures and in compliance with programme board decisions.

Decisions on nature of assessment will be linked to the need to achieve particular learning outcomes. They may be in the form of a written assessment, project or other relevant assessment. Individuals may be interviewed or asked to present their work in a formal student conference context to prove authenticity and ownership of work.

Indicative Coursework and Continuous Assessment:		**100 %**		
Form	***Title***	***Percent***	***Week (Indicative)***	***Learning Outcomes***
Assignment	Assignment 1	35 %	Week 6	1,2,3
Multiple Choice	Assignment 2 - Multiple Choice Questions	35 %	Week 13	1,2,3,4
Project	Project - Assess Compliance with Cyber Security Architecture Frameworks	30 %	Week 22	1,2,3,4,5

Full Time Delivery Mode Average Weekly Workload:			**4.00 Hours**		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Lecture	Weekly lecture and/or tutorial.	Flat Classroom	2	Weekly	2.00
Practical	Practical.	Computer Laboratory	2	Weekly	2.00

Online Learning Delivery Mode Average Weekly Workload:			4.00 Hours		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Online Learning	Online asynchronous delivery of content, via live & recorder webinars & interactions, video, audio and assignments.	Online	4	Weekly	4.00

Blended Delivery Mode Average Weekly Workload:			4.00 Hours		
Type	***Description***	***Location***	***Hours***	***Frequency***	***Weekly Avg***
Online Learning	Blended delivery of content, via live & recorder webinars & interactions, video, audio and assignments.	Online	3	Weekly	3.00
Online Learning	Monthly On Campus opportunity for group work/discussions/tutorials etc. In place of that weeks online delivery.	Not Specified	1	Weekly	1.00

Required Reading Book List
Stallings, W., (2018). *Effective Cybersecurity*. Addison-Wesley Professional. ISBN 0134772806 ISBN-13 9780134772806
Scott, S., (2015). *Enterprise Cybersecurity*. Apress. ISBN 9781430260837 ISBN-13 1430260831

Online Resources
https://www.nist.gov/cyberframework
http://www.isaca.org
http://www.isc2.org
http://www.nist.gov
http://www.sans.org
http://www.iso.org

Other Resources
Access to the Micrsoft Azure Platform.

Programme Membership
GA_KCYBC_L08 202000 Higher Diploma in Science in Cybersecurity Risk & Compliance