This Version is No Longer Current
The latest version of this module is available here

MODULE DESCRIPTOR

Module Title

Network Security

Reference	CMM402	Version	1
Created	April 2021	SCQF Level	SCQF 11
Approved	July 2021	SCQF Points	30
Amended		ECTS Points	15

Aims of Module

To enable the student to analyse network security threats and to design and manage secure networks.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Demonstrate a critical understanding of the principles of Secure Network Design.
2	Critically appraise the methods and technologies that can be used to protect networks against modern security threats.
3	Apply a range of specialised skills and techniques in designing a secure network to mitigate network attacks.
4	Apply a range of specialised skills and techniques in maintaining secure network operations to meet business requirements.

Indicative Module Content

OSI networking model. Network protocols and vulnerabilities. Managing a Secure Network: Principles of Secure Network Design and Security Policy implementation. Securing Network Devices: Secure administrative access to devices, secure management, monitoring and resiliency, security audit tools. Network protective measures, VLANs, Firewall Technologies, Access Control Lists (ACLs), Intrusion Detection and Prevention Systems (IDS/IPS), Virtual Private Networks (VPNs). Wireless Security. Advanced network security topics: IoT/OT Security, Software-Defined Network, Machine Learning for Intrusion Detection.

Module Delivery

The module is delivered via work-based learning along with structured online learning materials/activities and directed study, facilitated by regular online tutor support. Workplace Mentor support and work-based learning activities will allow students to contextualise this learning to their own workplace. Face-to-face engagement occurs through annual induction sessions, employer work-site visits, and modular on-campus workshops. Study Groups will be formed to encourage students to work collaboratively on set learning activities and share practice from their workplaces. Formative feedback will be provided to make sure teams are engaging positively and performing effectively.

Module Ref:	CMM402 v1

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	30	N/A
Placement/Work-Based Learning Experience [Notional] Hours	240	N/A
TOTAL	300	N/A
Actual Placement hours for professional, statutory or regulatory body	240	

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	50%	Outcomes Assessed:	1, 3
Description:	Report on building a secure network.				

Component 2

Type:	Coursework	Weighting:	50%	Outcomes Assessed:	2, 4
Description:	Report on analysing network security threats.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 50% weighting of C1 (X axis) and 50% weighting of C2 components (Y axis). An overall minimum grade D is required to pass the module.

		Coursework:						
		A	**B**	**C**	**D**	**E**	**F**	**NS**
Coursework:	**A**	A	A	B	B	C	E	
	B	A	B	B	C	C	E	
	C	B	B	C	C	D	E	
	D	B	C	C	D	D	E	
	E	C	C	D	D	E	E	
	F	E	E	E	E	E	F	
	NS	Non-submission of work by published deadline or non-attendance for examination						

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CMM402 v1

INDICATIVE BIBLIOGRAPHY

1	McNAB,C., 2016. Network Security Assessment. O'Reilly.3rd Ed.
2	RUSSELL, B., DUREN, D. V., 2018. Practical internet of things security: design a security framework for an internet connected ecosystem. Packt Publishing.
3	KIZZA, 2015. Guide to Computer Network Security. Springer.
4	STALLINGS, W., 2014. Network Security Essentials: Applications and Standards. Pearson.
5	ACKERMAN, P., 2017. Industrial cybersecurity: efficiently secure critical infrastructure systems. Packt Publishing.
6	TSUKERMAN, E., 2019. Machine learning for cybersecurity cookbook: over 80 recipes on how to implement machine learning algorithms for building security systems using Python. Packt Publishing.