This Version is No Longer Current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

MODULE DESCRIPTOR

Module Title

Information Security Management

Reference	CMM517	Version	2
Created	April 2018	SCQF Level	SCQF 11
Approved	January 2013	SCQF Points	15
Amended	June 2018	ECTS Points	7.5

Aims of Module

To enable the student to explore and critically appraise a wide spectrum of security concepts including information security management, cryptography and security services and enable them to analyse, assess the risks, design and implement a secure system in a given context.

Learning Outcomes for Module

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

1	Identify and discuss information security risks in a variety of environments.
2	Demonstrate an understanding of information security management requirements.
3	Apply and justify the use of appropriate cryptographic algorithms for the design and implementation of secure systems.
4	Select appropriate security services for a particular computer system.

Indicative Module Content

Security concepts: threats, vulnerabilities, and risk. Confidentiality, Integrity and Availability. Information security governance, policies, standards (e.g. ISO 27001), procedures and guidelines (e.g. Cyber Essentials). Security models. Security risk analysis and management. Security services: Authentication, Access Controls. Cryptography: symmetric and asymmetric encryption (AES, RSA, and Diffie-Hellman) and Hash Functions. Authentication systems: symmetric (Kerberos) and asymmetric (Certificates and Public Key Infrastructures) techniques. Crypto Systems (e.g. Secure Sockets Layer/Transport Layer Security).

Module Delivery

Key concepts are introduced and illustrated through lectures and directed reading. The understanding of students is tested and further enhanced through lab sessions.

Module Ref:	CMM517 v2

Indicative Student Workload	Full Time	Part Time
Contact Hours	44	44
Non-Contact Hours	106	106
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	150
Actual Placement hours for professional, statutory or regulatory body		

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:	2, 3, 4
Description:	This is a closed book examination.				

Component 2

Type:	Coursework	Weighting:	50%	Outcomes Assessed:	1
Description:	This is a coursework where the student will critically appraise the security of systems.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 50% weighting of C1 and 50% weighting of C2 components.

		Examination:						
		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 in addition to course entry requirements.
Corequisites for module	None.
Precluded Modules	None.

Module Ref:	CMM517 v2

INDICATIVE BIBLIOGRAPHY

1	NORMAN, T.L., 2016. Risk analysis and security countermeasure selection. CRC Press.
2	JACOBS, S. 2016. Engineering Information Security. Wiley.
3	GREGORY, P. 2018. CISM Certified Information Security Manager All-in-One Exam Guide. McGraw-Hill.
4	ALEXANDER,D.,FINCH,A.,SUTTON,D.,TAYLOR,A.,2013.Information Security Management Principles. British Computer Society.
5	CAMPBELL, G., 2014, The manager's handbook for business security. Elsevier.
6	SMART, N.P., 2015. Cryptography made simple. Springer.