MODULE DESCRIPTOR

Module Title

Information Security Fundamentals

Reference	CMM401	Version	2
Created	June 2022	SCQF Level	SCQF 11
Approved	July 2021	SCQF Points	30
Amended	July 2022	ECTS Points	15

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.

Learning Outcomes for Module

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

1	Critically analyse the risk landscape for an organisation.
2	Critically analyse the information security requirements of an organisation.
3	Critically appraise security controls to protect an organisation's assets.
4	Discuss the role of human factors in information security.

Indicative Module Content

Security concepts: threats, vulnerabilities, and risk. Security objectives: Confidentiality, Integrity and Availability. Information security governance, organisational/legal/regulatory context and compliance, policies, standards and guidelines. Security risk analysis and management. Information Security Management Systems (e.g., ISO 27001) and the Security Program. Planning for Contingencies. Human Factors: usable security, human error, security awareness and stakeholder engagement. Security services: Authentication and Access Controls (admin, technical and physical); Cryptography (symmetric and asymmetric encryption, hashing, digital certificates); Crypto Systems and Applications (e.g. TLS, Kerberos, Tor, crypto currencies).

Module Ref:	CMM401 v2

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.

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:	100%	Outcomes Assessed:	1, 2, 3, 4
Description:	Report on risk assessment and appraisal of security controls for a given scenario.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of C1. An overall minimum grade of D is required to pass the module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in C1.
B	The student needs to achieve a B in C1.
C	The student needs to achieve a C in C1.
D	The student needs to achieve a D in C1.
E	The student needs to achieve an E in C1.
F	The student needs to achieve an F in C1.
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:	CMM401 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. GREGOY, P., 2018, CISM Certified Information Security Manager All-in-One Exam Guide. McGraw-Hill.
4. WHITMAN, M.E., MATTORD, H.J., 2014. Management of information security. Cengage Learning.
5. CAMPBELL, G., 2014, The manager's handbook for business security. Elsevier.
6. AHRAM, T., KARWOWSKI, W., 2019. Advances in Human Factors in Cybersecurity. Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, July 24-28, 2019, Washington D.C., USA.
7. SMART, N.P., 2015. Cryptography made simple. Springer.