1. **Title of the module**

COMP8340 (CO834) – Information Security Management

1. **Division or partner institution which will be responsible for management of the module**

Division of Computing, Engineering, Mathematical Sciences (CEMS)

1. **The level of the module (Level 4, Level 5, Level 6 or Level 7)**

Level 7

1. **The number of credits and the ECTS value which the module represents**

15 credits (7.5 ECTS)

1. **Which term(s) the module is to be taught in (or other teaching pattern)**

Spring

1. **Prerequisite and co-requisite modules**

None

1. **The courses of study to which the module contributes**

Portfolio of Taught Postgraduate Courses in Computing, Engineering, Kent Law School, SSPSSR, and Kent Business School

1. **The intended subject specific learning outcomes.  
   On successfully completing the module students will be able to:**

8.1 Demonstrate systematic understanding and critical awareness of the importance of taking a systems-wide approach to maintaining cyber security, and the role of information security policies including those for security risk management.

8.2 Comprehensively understand the motivation, design, operation, and management of modern systems for security management, including awareness of relevant human factors especially usability issues.

8.3 Show appreciation of legal issues on security and data protection, and relevant security (management) standards.

8.4 Analyse and evaluate critically the security and data protection legal requirements of an organisation.

8.5 Demonstrate systematic understanding of appropriate processes, techniques, and tools for developing and managing security systems.

8.6 Understand the basis of business continuity planning and management, and cyber resilience.

1. **The intended generic learning outcomes.  
   On successfully completing the module students will be able to:**

9.1 Demonstrate critical thinking, reasoning, and reflection.

9.2 Produce a specification of the operation of a complex system based on an understanding of the component parts.

9.3 Undertake critical appraisal of a candidate system design and reflect upon its merits and drawbacks.

9.4 Able to select, justify and reflect on choices.

9.5 Manage time and resources within a potentially complex problem domain.

1. **A synopsis of the curriculum**

This module investigates the whole process of information security management and associated activities including the concepts used and practices prescribed by relevant standards, such as those defined by ISO/IEC. A holistic view of information security management is taken, including risk management, the formulation of security policies, business continuity and resilience.

Selected socio-technical topics that are important for information security management will also be covered. These shall include AAA (authentication, authorisation and accountability), important legal aspects especially data protection and privacy laws, data protection impact assessment, usability analysis and management, wider human factors in cyber security such as social engineering attacks and the importance of a positive cyber security culture for encouraging secure behaviours of employees and users.

1. **Reading list (Indicative list, current at time of publication. Reading lists will be published annually)**

Taylor, A., Alexander, D., Finch, A. and Sutton, D., “Information Security Management Principles”, 2019, 3rd edition, BCS.

Calder, A. and Watkins, S., “IT governance: an international guide to data security and ISO27001/ISO27002”, 2019, 7th edition, Kogan Page.

Sutton, D., “Information Risk Management: A practitioner’s guide,” 2014, BCS.

Burnap, P., “Risk Management & Governance,” Version 1.1.1, 2021, <https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf>

Carolina, R., “Law & Regulation,” Version 1.0.2, 2021, <https://www.cybok.org/media/downloads/Law_Regulation_v1.0.2.pdf>

Troncoso C., “Privacy & Online Rights,” Version 1.0.2, 2021, <https://www.cybok.org/media/downloads/Privacy_Online_Rights_v1.0.2.pdf>

Sasse, M.A., and Rashid, A., Human Factors, Version 1.0.1, 2021, <https://www.cybok.org/media/downloads/Human_Factors_v1.0.1.pdf>

Debar, H., “Security Operations & Incident Management,” Version 1.0.2, 2021, <https://www.cybok.org/media/downloads/Security_Operations_Incident_Management_v1.0.2.pdf>

Gollmann, D., “Authentication, Authorisation & Accountability,” Version 1.0.2, 2021, <https://www.cybok.org/media/downloads/Authentication_Authorisation_Accountability_v1.0.2.pdf>

Further readings are provided with each lecture.

1. **Learning and teaching methods**

Total contact hours: 30

Private study hours: 120

Total study hours: 150

1. **Assessment methods**
   1. Main assessment methods

Timed Moodle Quiz (20%)

Mini-Project (30%, approximately 15 hours)

Written examination, 2 hours (50%)

13.2 Reassessment methods

Like for like.

1. **Map of module learning outcomes (sections 8 & 9) to learning and teaching methods (section12) and methods of assessment (section 13)**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Module learning outcome** | **8.1** | **8.2** | **8.3** | **8.4** | **8.5** | **8.6** | **9.1** | **9.2** | **9.3** | **9.4** | **9.5** |
| **Learning/ teaching method** |  |  |  |  |  |  |  |  |  |  |  |
| Lectures | **x** | **x** | **x** | **x** | **x** | **x** | **x** |  |  | **x** |  |
| Seminars | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** |
| Private Study | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** |
| **Assessment method** |  |  |  |  |  |  |  |  |  |  |  |
| Written examination | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** |  |
| Mini-Project | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** |
| Timed Moodle Quiz | **x** | **x** | **x** |  | **x** | **x** | **x** | **x** | **x** | **x** | **x** |

1. **Inclusive module design**

The Division recognises and has embedded the expectations of current equality legislation, by ensuring that the module is as accessible as possible by design. Additional alternative arrangements for students with Inclusive Learning Plans (ILPs)/declared disabilities will be made on an individual basis, in consultation with the relevant policies and support services.

The inclusive practices in the guidance (see Annex B Appendix A) have been considered in order to support all students in the following areas:

a) Accessible resources and curriculum

b) Learning, teaching and assessment methods

1. **Campus(es) or centre(s) where module will be delivered**

Canterbury

1. **Internationalisation**

Most of the curriculum in this module is universal in its scope. The module focuses for the most part on technology and international standards which apply worldwide. Where the module does touch on legal aspects, care is taken to specify which issues apply solely to the UK or EU, and which apply more universally.

**DIVISION USE ONLY**

**Revision record – all revisions must be recorded in the grid and full details of the change retained in the appropriate committee records.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date approved | Major/minor revision | Start date of the delivery of revised version | Section revised | Impacts PLOs (Q6&7 cover sheet) |
| 03/12/19 | Major | September 2020 | 1, 6-8, 10-14 | No |
| 04/12/2020 | Major | September 2021 | 1,8,9,10,11,13 | No |
| 11/04/2022 | Major | September 2022 | 8-14 | No |