# Programme Specification

**Postgraduate**

Applicable to postgraduate programmes

Please click [here](#) for guidance on completing this specification template.

## Part A: Programme Summary Information

1. **Title of programme:**  
   - Cyber Security Compliance Management

2. **Programme Code:**  
   - 

3. **Entry Award(s):**
   - **Credit:**  
     - **Level:**  
     - [ ] MA  
     - [ ] MSc  
     - [ ] PGDip  
     - [ ] PGCert  
     - [x] PG Award  
     - [ ] DPS  
     - [ ] CPS  
     - [ ] Other (please specify below):  
       - 

4. **Exit Awards:**
   - **Credit:**  
     - **Level:**  
     - [ ] PGDip  
     - [ ] PGCert  
     - [ ] PG Award  
     - [ ] CPS

   Exit awards will automatically bear the name of the entry award. If an exit award is to be unnamed (i.e. it will show only the qualification achieved) or if it is to have a different name from the entry qualification you must indicate this below:

   - 

5. **Date of first intake:**  
   - May 2017
6. Frequency of intake: 4-6 times per academic year depending on demand

7. Duration and mode of study: Part-time 2 years
   The mode of study is by online learning

8. Applicable framework: University Framework for Postgraduate Modular Provision
   Framework exemption required: ☒ No (please go to section 9)
   ☐ Yes (please provide a brief summary below)

Date exemption approved:

9. Applicable Ordinance: General Ordinance for Modular Master’s Degrees, Postgraduate Diplomas, Postgraduate Certificates and Postgraduate Awards.
   New/revised Ordinance required: ☒ No (please go to section 10)
   ☐ Yes (please provide a brief summary below)

Date new/revised Ordinance approved by Council:

10. Faculty: Faculty of Science and Engineering

11: Level 2 School/Institute: School of Electrical Engineering, Electronics and Computer Science

12. Level 1 unit: Department of Computer Science

13. Campus:

14. Other contributors from UoL:

15: Teaching other than at UoL: Laureate Online Education

16: Director of Studies: Professor Frans Coenen

17: Board of Studies: Computer Science Board of Studies (Online)

18: Board of Examiners: Board of Examiners for Online Degrees in Computing
**Part B: Programme Aims & Objectives**

**26. Aims of the Programme**

The PG Award in Cyber Security Compliance Management is specifically designed to meet employment and career opportunities available with respect to security risk management, and security engineering and compliance. The programme is intended to meet the needs of those already working in the field of data security who wish to enhance their current understanding in the context of security compliance management. The programme is also intended for those who wish to move into this field so as to broaden their capabilities. The programme incorporates both theoretical and practical aspects of security engineering compliance and risk management.

**No.  Aim:**

1. **To provide students with a comprehensive understanding of the theoretical underpinning that supports security engineering compliance and risk management.**
To provide students with a critical understanding of the challenges in assessing and managing security risks within the modern workplace.

To provide students with an opportunity to create a professional development plan and, throughout the course of the programme, build an E-Portfolio that exhibits their understanding of Cyber Security Compliance Management.

**Learning Outcomes**

**No.** Learning outcomes – Master’s degree

**Learning Outcomes**

**No.** Learning outcomes – Postgraduate Diploma

**Learning Outcomes**

**No.** Learning outcomes – Postgraduate Certificate

**Learning Outcomes**

**No.** Learning outcomes – Postgraduate Award

1. A comprehensive understanding of the role of security engineering, and cyber security compliance, within the context of the modern workplace.

2. An in depth and critical knowledge of the management processes that can be deployed to prevent/limit potential cyber-attacks and how these processes can be deployed in the workplace.

**Mapping of subject-based learning outcomes:**

<table>
<thead>
<tr>
<th>Learning outcome No.</th>
<th>Module(s) in which this will be delivered</th>
<th>Mode of assessing achievement of learning outcome</th>
<th>PSRB/Subject benchmark statement (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CKIT511</td>
<td>Practical assessments/Reports Discussion Questions</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>CKIT531</td>
<td>Practical assessments/Reports Discussion Questions</td>
<td></td>
</tr>
</tbody>
</table>

**Skills and Other Attributes**

**No.** Skills and attributes:
1. A systematic understanding of the process of Online Learning and its significance with respect to independent learning and continuing professional development.

2. The ability to present and communicate professional concepts to colleagues and clients.

### 28a. Mapping of skills and other attributes:

<table>
<thead>
<tr>
<th>Skills and other attributes No.</th>
<th>Module(s) in which this will be delivered and assessed</th>
<th>Learning skills, research skills, employability skills</th>
<th>Mode of assessing achievement of the skill or other attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Online Learning features throughout the programme</td>
<td>Learning</td>
<td>Practical, Written</td>
</tr>
<tr>
<td>2</td>
<td>CKIT511, CKIT531</td>
<td>Employability</td>
<td>Practical, Written</td>
</tr>
</tbody>
</table>

### 29. Career opportunities:

Cyber security is a rapidly expanding field within the umbrella domain of Computer Science, and has been identified as an “in-demand” skill. Market research indicates an increasing commercial spend on information security. The CPD Award in Cyber Security Compliance Management seeks to address the skills shortages in the field of cyber security, particularly with respect to compliance management. The programme will provide a mechanism whereby students can upgrade their skills with a view to future compliance management employment opportunities. Industries where such positions will be available include all industries that routinely store/handle/collate data using computers; within the commercial and financial sectors as well as within technical domains such as big data, data management and warehousing and cloud computing. More generally the programme seeks to provide students with skills that are currently in great demand and will continue to be in demand.

### Part C: Entrance Requirements

#### 30. Academic Requirements:

Either a first degree in Computer Science, or some similar numeric subject, equivalent to a UK Bachelor’s degree, coupled with 2 years relevant IT professional experience; or such experience in IT employment as would be considered to be comparable with the award of a Bachelor’s degree.

Applications from students with a professional IT background, rather than a Bachelor’s degree, will be assessed in accordance with established practice for the University of Liverpool’s online Computer Science programmes that are delivered in collaboration with Laureate Online Education, as follows:

1. At least three years’ experience for holders of the equivalent of an HNC/HND (or 2 years certified HE).
2. At least five years’ experience for holders of the equivalent of GCE A-levels or an ONC/OND.
3. At least ten years of experience otherwise.
The initial contact for applicants will be a representative of Laureate Online Education. The final decision as to whether to admit an applicant to the programme lies with the Department of Computer Science at the University of Liverpool.

31. **Work experience:**

   For graduates (as noted above) normally two years’ work experience in IT-related employment is required; a significantly longer period of relevant employment is necessary for candidates lacking a first degree.

32. **Other requirements:**

   English-language skills equivalent to at least IELTS 6.5.

### Part D: Programme Structure

33. **Programme Structure:**

   1. **Programme Structure**

      All modules are at level 7.

   1.1 **PG Award Cyber Security Compliance Management (Entry Award)**

      The modules in the PG Award Cyber Security Compliance Management programme are as follows:

      **Mandatory modules:**
      1) CKIT511 Security Engineering and Compliance (15 credit points)
      2) CKIT531 Security Risk Management (15 credit points)

34. **Industrial placement/work placement/year abroad:**

   Not applicable

35. **Liaison between the Level 2 Schools/Institutes involved:**

   Delivery of the programme is undertaken by the Department of Computer Science at the University of Liverpool in partnership with Laureate Online Education. Staff within the Department of Computer Science liaise regularly with colleagues at Laureate who are responsible for the day-to-day management of the programme. The University retains control over all academic aspects of the programme and its delivery. Appropriate Laureate personnel are represented on the Board of Studies and Board of Examiners, together with representatives of the Department of Computer Science.

### Part E: Learning, Teaching and Assessment Strategies

36. **Learning, Teaching and Assessment Strategies:**
The mode of delivery of taught modules is by internet facilitated distance learning. This mode of study enables students to pursue modules via home study while continuing in employment.

Module delivery involves the establishment of a virtual classroom in which a relatively small group of students (usually 15-20) work under the direction of a module instructor, using an internet-based distance learning package. Module delivery proceeds via a series of one-week online seminars, each of which typically includes:

1. An online lecture, and other learning materials, posted electronically to a public folder in the virtual classroom.
2. Coursework assignments, which may include both reading assignments and practical work, results from which are posted to closed folders in the virtual classroom.
3. Class discussions and group assignments, facilitated and moderated by the class instructor, carried out within open folders.

Communication within the virtual classroom is asynchronous, preserving the requirement that students are able to pursue the course in their own time, within the weekly time-frame of each seminar.

Two broad principles inform the teaching and learning strategy: social constructivism and collaborative enquiry. Social constructivism describes a view of learning in which students construct their own unique understanding of a subject, through a process which includes social interaction so that the learner can explain understandings, receive feedback from teachers and other students, clarify meanings, and reach a group consensus. Collaborative enquiry via Internet-mediated communication provides a framework for this mode of learning. The aim is to use the medium to foster the creation of a learning community, which will enable: dialogue between participants, sharing of information, and collaborative project work. This mode of learning is particularly appropriate when, as in this case, the students themselves will often bring knowledge and expertise that is outside the experience of the course teacher, and which can be shared with the group.

A key feature of the approach is the use of moderated discussions of material introduced in the virtual classroom. Every taught module includes, each week, a discussion of topics specified by the instructor. Participation in these discussions is a requirement for students attending, and forms part of the basis for assessment. This requirement ensures a continuing commitment from the students to the learning process.

All communications that take place within the virtual classroom, including all assignments carried out by students and assessments by instructors, are recorded and are available for scrutiny by staff with appropriate access permissions. This enables two aspects of quality control:

1. Module delivery is monitored by staff at the Department of Computer Science to ensure that defined syllabuses, procedures, and assessment processes are followed, appropriate standards are maintained, and to check for plagiarism.
2. All assessments are subject to the Universities moderating procedures.

All assessment is subject to inspection by external examiners.
Under normal circumstances students will be expected to take the two modules one after the other. Under special circumstances students can apply to the Director of Studies to take both modules at the same time. However, students who do so should be clear that taking two modules at the same time cannot be used as grounds for an extenuating circumstances claim.

36a. **Learning, Teaching and Assessment methods:**

Assessment is entirely based on work carried out in the virtual classroom, including contribution to discussions, weekly assignments, and longer individual or group-based projects. The weighting assigned to each component is prescribed separately for each module. The main aim of the assessment strategy is to verify the achievement of learning outcomes within the broad framework of the degree classification, thus at Pass, Merit and Distinction levels.

37. **Assessment information for students:**

**Code of Practice on Assessment**

The University has a Code of Practice on Assessment which brings together the main institutional policies and rules on assessment. The Code is an authoritative statement of the philosophy and principles underlying all assessment activities and of the University's expectations in relation to how academic subjects design, implement and review assessment strategies for all taught programmes of study.

The Code of Practice includes a number of Appendices which provide more detail on the regulations and rules that govern assessment activity; these include:

- The University marks scale, marking descriptors and qualification descriptors;
- The framework for modular, postgraduate programmes;
- Information about students’ progress, including guidance for students;
- The procedure for assessment appeals;
- Regulations for the conduct of exams;
- The University’s policy on making adjustments to exam arrangements for disabled students;
- The code of practice relating to external examining (see also below);
- The Academic Integrity Policy, which covers matters such as plagiarism and collusion and includes guidance for students;
- The policy relating to mitigating circumstances which explains what you should do if you have mitigating circumstances that have affected assessment; and
- The policy on providing students with feedback on assessment.

Please click [here](#) to access the Code of Practice on Assessment and its appendices; this link will also give you access to assessment information that is specific to your cohort:

A summary of key assessment information is also available in the ‘Your University’ handbook.

**Marking criteria:**

Taught modules are typically eight weeks in duration. Typically students receive grades for several units of assessment carried out each week. Grading is founded on a six-point scale: A* A B C D F. The grade descriptors...
to be used in association with this six-point scale are presented in Table 1 below. These grades are converted into a weighted average final mark (expressed as a percentage) for each module. These final module marks will then be used to determine the degree award and for inclusion in transcripts. The weightings given to each component making up individual modules are specified in the module specifications.

<table>
<thead>
<tr>
<th>Grade</th>
<th>Description</th>
<th>Numerical Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A*</td>
<td>High Distinction-level work: Factually almost faultless; authoritative coverage of topic; strong evidence of outside reading/research; substantial elements of originality and independent thought. Perceptive; aptly focused; very well written and directed. Exceeds requirements.</td>
<td>84%</td>
</tr>
<tr>
<td>A</td>
<td>Distinction-level work: Displays in-depth understanding of material; comprehensive coverage of topic; good evidence of outside reading/research; originality of thought or approach. Enlightening; well-focused; very well written and directed. Exceeds most expected requirements.</td>
<td>74%</td>
</tr>
<tr>
<td>B</td>
<td>Merit-level work: Factually sound (few, if any, minor factual errors); thorough understanding of material; evidence of relevant outside reading/research; some originality of thought or approach. Regular use of effective logical thinking, critical analysis and judgment. Suitably focused; well written and directed. Meets all expected requirements.</td>
<td>64%</td>
</tr>
<tr>
<td>C</td>
<td>Pass-level work: Essentially correct, possibly missing important points, but no serious errors; good understanding of material but tending to be descriptive in approach; limited evidence of outside reading/research. Competently structured and reasonably well focused, but some weaknesses in expression/presentation. Possibly using large amounts of quotations. Meets most expected requirements.</td>
<td>54%</td>
</tr>
<tr>
<td>D</td>
<td>Marginal work: Displays only limited understanding of material; incomplete coverage of topic; some significant factual errors and/or irrelevancies. Entirely descriptive in approach. Poorly structured; lack of coherent argument; difficult to follow. Substantially above or below the word limit. Possibly using excessive amounts of quotations. Meets some of the expected requirements but not all.</td>
<td>44%</td>
</tr>
<tr>
<td>F</td>
<td>Unsatisfactory work: Evidence of inadequate effort. Many serious errors / misconceptions / omissions / irrelevancies. Poorly directed at targets. Poorly structured; lack of coherent argument; difficult to follow. Substantially above or below the word limit. Possibly using excessive amounts of quotations.</td>
<td>0%</td>
</tr>
</tbody>
</table>
Table 1: Grade Descriptors

**Pass marks**
The pass mark for each module is 50%.

**Re-takes**
Marks achieved through re-assessment will be capped at 50% for the purposes of calculating the overall mark and determining classification for an award; The actual mark achieved through reassessment will be the mark recorded on the transcript.

**Final awards**

A *Postgraduate Award in Cyber Security Compliance Management (Entry Award)* will be awarded to students who achieve a minimum of 30 credit points as per the prescribe programme of study detailed in this programme specification.

A mark of Merit or Distinction will be awarded according to the criteria set out in the University’s code of practice on assessment.

There is no provision for an exit award should a student fail to complete the programme.

### 38. Student representation and feedback:

Because of the nature of the delivery of the programme, and the world-wide distribution of the student body enrolled on the programme, physical participation in a Liverpool-based Staff-Student Liaison Committee (SSLC) is impracticable. Instead SSLCs, run on similar lines as on-campus SSLCs, are conducted in the form of teleconferences. SSLCs are held three times a year prior to each Board of Studies (BOS) meeting. Each BOS receives a report from its associated SSLC, these reports are also posted online. Feedback from each BOS is provided at each subsequent SSLC.

The principal channel for students to communicate with their colleagues and with staff, in keeping with the medium for programme delivery, is the Internet. Each module delivered establishes a virtual classroom within which the module instructor will communicate with students to deliver module materials, receive coursework assignments and facilitate class discussions. This mechanism automatically provides a framework for students to share concerns with their colleagues and with staff, either privately or publicly, within the class. Other concerns can be raised privately via the student’s Student Support Manager (SSM). Each student is assigned, for the duration of his/her studies, a Laureate based SSM whose role includes that of acting as a personal tutor.

Feedback on the delivery of individual modules is provided through the completion of a “end of module” questionnaire issued to all students taking part in the module. A summary of the questionnaire returns is given to the module instructor, who is asked to comment on this, and any other issues arising in the delivery of the module, in the form of a report with prescribed headings. This report may be further augmented by comments from a member of UoL staff (the module monitor). Each module delivery is reviewed by the Board of Studies, which is provided with the composite module report, including the questionnaire summary. An overall summary of student feedback is also presented for consideration at each meeting of the
Board of Studies. These reports are also made available to the Board of Examiners.

### Part F: Status of Professional, Statutory or Regulatory Body Accreditation

#### 39. Status of Professional, Statutory or Regulatory Body Accreditation:

The British Computer Society (BCS), the body that accredits most Computer Science UG and PG taught programmes in the UK, does not accredit PG Awards.

### Part G: Diversity & Equality of Opportunity and Widening Participation

#### 40. Diversity & Equality of Opportunity and Widening Participation:

The programme design, structure and content are consistent and compliant with the University’s Diversity and Equality of Opportunity Policy.

### ANNEX 1

**Annex Of Modifications Made To The Programme**

Please complete the table below to record modifications made to the programme.

<table>
<thead>
<tr>
<th>Description of modification (please include details of any student consultation undertaken or confirm that students’ consent was obtained where this was required)</th>
<th>Minor or major modifications</th>
<th>Date approved by FAQSC</th>
<th>Date approved by AQSC (if applicable)</th>
<th>Cohort affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Programme</td>
<td>Not Applicable</td>
<td>February 2017</td>
<td>March 2017 (UAP)</td>
<td>May 2017</td>
</tr>
</tbody>
</table>