OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TECHNOLOGICAL UNIVERSITY DUBLIN

SCHOOL OF INFORMATICS & ENGINEERING

PROGRAMME VALIDATION REPORT

TU252X Postgraduate Diploma in Cybersecurity (NFQ Level 9, 60 ECTS)

TU5352 Postgraduate Certificate in Cybersecurity (NFQ Level 9, 30 ECTS)

Blanchardstown Campus,
Blanchardstown Road North, Dublin 15,
D15 YV78

https://www.tudublin.ie **[to insert programme link here if available]**

Review Panel Date (Desktop Validation Deadline): June 10, 2022

Introduction

The (TU252) MSc in Computing in Applied Cyber Security (90 ECTS credits) currently has exit awards of PG Certificate (30 ECTS credits) and PG Diploma (60 ECTS credits). However, the programme now wishes to offer the Postgraduate Certificate and Postgraduate Diploma programmes as entry level programmes to complement the masters programme offering.

The rational for having the two entry programmes is due to the demand from industry for specialised courses that can be used for up-skilling and re-skilling of employees and having progression opportunities leading to higher qualifications. This has been stated in many Government and Industry reports.

The new entry level Postgraduate Diploma in Cybersecurity will allow companies to partnership with TU Dublin in providing education and training in specialist areas of cybersecurity that would be suitable for individual companies. These specialist training courses can be linked to specialist job roles within the company and thus allowing for employee redeployment to skill needs areas. The Postgraduate Diploma packages together already accredited modules from the (TU252) MSc in Applied Cyber Security degree and offer them as a 60-credit independent award. In general, the rational is based on the demand from industry for shorter specialised courses that can be used for training employees while still having progression opportunities leading to higher qualifications.

The PG Certification will be an example of Excellence, Practice-Led, impact focused and co-creation by:

- providing a student-centred learning experience that is supporting the growth of enterprising and socially responsible professionals in cybersecurity knowledge and skills.
- the course is very practice-led and has strong impact-focused engagement that is addressing a national and international crisis in talent supply in a critical skill-needs area of cybersecurity.
- course content and delivery, in partnership with stakeholders and customers, to achieve a co-creation space in achievement of the proficiency levels and competencies needed for cybersecurity job roles for now and the future.

VALIDATION PANEL MEMBERS

Member(s): Higher Education Sector

Professor Kevin Curran
School of Computing, Engineering & Intelligent Systems
Faculty of Computing, Engineering & the Built Environment
Ulster University, Magee College, Derry, Northern Ireland
See Profile at: https://kevincurran.org

Professor Donna O'Shea,
Chair of Cybersecurity,
Munster Technological University, Cork
See Profile at: https://www.linkedin.com/in/donna-o-shea/?originalSubdomain=ie

Member(s): Senior Business/Industry Expert:

Mr David McNamara,
CommSec,
Suite B109, The LINC, Technological University Dublin, Blanchardstown,
See Profile at: https://www.linkedin.com/in/david-m-2785a72/

Ms. Ann Duignan,
Cyber Security Manager, Accenture
Address: 63 Ashbrook, Howth Road, Clontarf, D3 (D03VP03)
See profile at: https://www.linkedin.com/in/ann-duignan-49341421

Guidelines for Validation/Review Panel

In assessing the proposal in this programme/module review, the panel considered the guidelines per section headlines below.

1. Title

Is the title of the proposed programme/module clear, accurate and fit for the purpose of informing prospective learners and other stakeholders?

The title of the proposed programme is appropriate, clear, and accurate. It draws from the MSc Major Award in which both Postgraduate Diploma and Postgraduate Certificate are Exit Awards.

2. Award NFQ level and ECTS credits

Is the NFQ level of the award and ECTS credits as proposed appropriate?

The existing MSc in Computing in Applied Cyber Security (TU252) is a 90 ECTS credit programme that already considers exit awards of Postgraduate Certificate (30 ECTS credits) and Postgraduate Diploma (60 ECTS credits). Therefore proposal is appropriate.

3. Learning outcomes

- Will the learning outcomes as proposed in the changes provide a valuable learning experience within a cohesive, logical structure worthy of this minor award?
- Do the proposed changes alter the overall programme learning outcomes of this minor award?

3.1 The learning outcomes of the proposed programmes are achieved through the application of a range of teaching and learning methods, including authentic learning pedagogy with authentic assessments. Authentic learning refers to educational and instructional techniques that focus on connecting what students are taught in school to real-world issues, problems and applications.

3.2 Lectures, workshop exercises, tutorials and project work pertinent to each module will be delivered in a structured manner. Primarily, each module will aim to introduce the students to the fundamentals and concepts of the subject area. Instruction will then advance to an appropriate level to cover in-depth knowledge, to foster development of individual aptitudes and competence, and (where relevant) to develop team-working skills in the respective areas. There will be individual and group workshop and tutorial assignments, problem solving and project work including visits from industry representatives in the mode of guest speakers. Where it is possible and relevant, case studies across the various modules will be encouraged.

3.3 Course projects will be based on selected real world situations for the students to engage. This will give the projects a realistic flavour and allow the student to appreciate the skills they need to be effective problem-solvers. The final dissertation will give students responsibility for a substantial piece of independent work conducted at level 9 including independent research of a topic, and demonstrating an ability to conceptualize that research and analyze their results.

3.4 The learning outcomes as proposed will provide a valuable learning experience. However, it remains unclear whether some of the learning outcomes can be achieved with the topics that are proposed. For example, a learning outcome states that the student will have “an acute understanding of risk management”. (PG-Diploma: P4 , PG-Certificate: P3). It is unconvincing that this can be achieved as there is no module covering risk management in a comprehensive manner. Although it is covered in topics such as Business Continuity, it is unclear how much time/emphasis is laid on the subject of Risk Management.

3.5 The programmes as proposed will be valuable for industry as there is a major shortage in Cybersecurity skillset. The proposed programmes will also enable and support students who are already in full time employment to upskill in Cyber Security.

4. Core values, mission and strategy

Is the proposed programme in unison with the core values and mission of TU Dublin, to embrace a policy of inclusion and participation in third level education?

The programme is aligned with the strategy of the Department which aims:

- to provide relevant high quality educational programmes to the community and enterprise industry within the catchment area.
- to be known for excellence in teaching and research.
- to have high quality collaboration with enterprise class industry and other 3rd level institutions.
- to continually enhance the student learning experience.
- Variable routes for access and progression.

Overall, the proposed programme is in unison with the core values and mission of TU Dublin.

5. Demand

Has a demand for the proposed programme been identified and has evidence been provided to support same?

5.1 The rationale for proposing the Postgraduate Cert and Postgraduate Diploma programmes, is mainly due to the demand from industry. Many Government and Industry reports, advocate for specialised courses that can be used for up-skilling and re-skilling of employees, with clear progression opportunities leading to higher qualifications.

5.2 There is a strong rationale, therefore, corresponding demand would be expected. However, it is unclear if the programmes are delivered online/remotely or face-to-face on campus. This should be made clearer under the delivery mode section of the programme documentation.

5.3 There was no formal evidence/data provided to quantify the demand for the programme. However, as the panel members work in the industry, they have first-hand feel for the demand for cyber security skills. Therefore, these specialised courses, provide potential students will have additional options for gaining cyber security skills, which is a positive step.

6. Entry requirements

Are the entry requirements clearly articulated and fit for purpose?

6.1 The entry requirements are specified clearly and are appropriate (Section 1.8 of submission document).

6.2 The minimum entry requirement for standard entrants to the PG-Certificate and PG-Diploma is 2nd Class Honours Grade 2 (GPA 2.5 or equivalent), in an NFQ Level 8 Degree in Computing, Science, Engineering, Business with IT, or equivalent. The acceptance of candidates with third class honours degrees and appropriate work experience and industrial certification on this course will be allowed, provided there is evidence that the candidate can cope with the learning objectives of the course. Candidate will be interviewed to assess their suitability to undertake the level work required and to assess their commitment to succeeding on the Postgraduate programmes. These entry requirements form the mandatory prerequisites for each of the modules in the syllabus.

6.3 The documentation would be improved by linking to the relevant TU Dublin RPL/WBL policies.

6.4 There was view expressed that entry should be restricted to graduates of Computing courses only, since Cybersecurity is a technical field of study, and the student needs to have a solid understanding of IT concepts to excel.

7. Access, transfer and progression

Have procedures for access, transfer and progression been incorporated?

7.1 Candidates that successfully complete the Postgraduate Cert can register on the Postgraduate Diploma and take three more modules to complete the 60-credits required for this award. There are number of different routes to progress to the Masters programme:

a. Candidates that successfully complete the PG-Cert have two choices:

i. They can take a 60-credit project or

ii. They can transfer to the master's programme where they need to take 3 more 10-credit modules and the 30-credit project.

b. Candidates that successfully complete the PG-Diploma need to take a bridging module in Research Skills & Ethics before transferring to the master's programme to take the 30-credit project. This module is a mandatory requirement on the master's programme.

7.2 The diagram on page 14/25 is unclear if learners can take the research skills module as part of the progression route from the Certificate to MSc via the 60-credit project.

7.3 It is specified that if you complete the Postgraduate Diploma to 30 credit project, the students will have to take a bridging module, but it is not clear if this bridging module is credit bearing.

8. Standards of knowledge, skill or competence

- Does the proposed programme/module meet the required QQI Award Standards as appropriate to the proposed NFQ level?
- Will learners be able to attain the standard of knowledge, skill or competence as presented?

8.1 The proposed programme meets the required QQI Award Standards as appropriate to the proposed NFQ level. It is clear that learners will be able to attain the standard of knowledge, skill or competence as presented.

8.2 Programme Outcomes for the Postgraduate Diploma indicates that a greater depth of knowledge is acquired as defined clearly in PO1. The Postgraduate Diploma also expects the learner to reflect on their own CPD and learner needs as defined in PO6. There are several module LOs that map to PO6, e.g., Security Intelligence, Cyber Crime Malware and Application Security. Also, for the Postgraduate Diploma, the learner can choose 6 out of 8 possible modules, to form part of the final award. However, it is rather unclear/uncertain whether PO6 will be sufficiently covered if students decide not to take modules that do not map to this Programme Outcome.

8.3 Programme team to consider reviewing the "Cyber Risk Specialist" option on the Postgraduate Certificate. The title suggests an emphasis on risk management, but none of the modules are focused on risk management. Each of them as an element of risk, but given the title of the option, one would expect a module focused on risk management. The other two options have modules that relate directly to the title, but the "Cyber Risk Specialist" doesn't have that.

8.4 The Secure Programming module should be reconsidered. Without a background in software development, it could be hard for students to grasp the concepts of writing secure code. The panel noted that even experienced Security Professionals struggle with this.

8.5 There are some topics not covered, but which are important and need further consideration. For example, Vulnerability Management and Access Control are critical for any organisation to implement and are part of most security industry standards such as ISO 27001, CIS and NIST.

8.6 The three specialist subject clusters of, Development Specialist, Forensics Specialist and Cyber Risk-Specialist, provide useful categorisation of related knowledge and experience for potential future employers.

9. Teaching and learning

Have the teaching and learning strategies of the proposed programme/module been clearly articulated?

9.1 The teaching and learning strategies of the proposed programme have been clearly articulated.

9.2 The department of Informatics has 40 lecturers and approximately 900 FTE students. Two main ICT undergraduate degrees are delivered in full-time mode;

- BSc (hons) in Computing in Information Technology and BSc (hons) in Computing in Digital Forensics & Cyber Security and courses from level 6 to 9 for part-time students.
- The referred degree programmes have multiple access routes through a two year higher certification, three year ab initio and one year add-on courses for years 3 and 4.
- The programmes currently accept 150 students from CAO each year into year 1 and allows for advanced entry into year 2 from Colleges of Further Education.
- Other routes onto full-time courses have come from Springboard and ICT Skills initiatives and from international students and Erasmus students.

9.3 Continuous assessment is used as a teaching method assessing learning as it is occurring, the focus being on constructive learning where feedback is motivational and directed at improvement.

9.4 Summative assessment is used to assess learning against expected outcomes, typically on module completion. There is a table giving details of the contact-hours to be devoted to each subject in terms of the breakdown of this between laboratory, practical, workshops, studio, tutorials, lectures. The staff member(s) to deal with each subject is listed.

10. Learner assessment

- Has a programme/module assessment strategy been provided?
- Is the method and scale of learner assessment appropriate and adequately described?

10.1 The method and scale of learner assessment is appropriate and has been adequately described within the submission document. The programme assessment method has been described.

10.2 Assessment procedures include a combination of in-class tests, formal examinations, assignments, reports, project presentations and seminars. Where appropriate, both theoretical and experimental techniques are covered, including the enhancement of skills in verbal and other communication, and technical reporting in both written and oral formats. These skills are often listed as desirable by employers as well as their technical skills requirements.

10.3 The authentic assessments mirror the tasks and problem solving that are required in reality. Where possible, projects will be “real-world” based and the involvement of experts from industry will be engaged for guidance and feedback to students. This will hopefully give the students experience of dealing with industry based people and expose them to the expectations of real-world project deliverables. Involvement of industry people in student presentation of project work will also act to give us feedback on the course itself.

10.4 The reporting skills will also reflect that the students are studying the necessary communication skills. Coursework assessment for respective course modules where appropriate, will include individual and teamwork assignments and projects in form of class and laboratory exercises, workshop practice, and assignments.

11. Resources

Are the necessary resources and facilities required to deliver the proposed programme available within the Institute?

11.1 The facilities are appropriate to enable an evaluation to take place of laboratories and other accommodation facilities to be available to learners participating in this programme.

11.2 The panel noted that the specialist equipment and software required was already in use by the current courses, therefore, there would be minimal additional resources implications.

11.3 The panel recommends addition of the following elements for programme enhancement, particularly, awareness of graduates of the programmes:

- Adding information on Security Frameworks (e.g., NIST, ISO, GDPR) as part of recommended resources if not covered in modules. It was noted that NIST is mentioned as a recommended resource, however, this is for the Biometrics module which is not part of the 3 proposed clusters.
- Incorporate new regulations into relevant areas. For example, clients are constantly asking questions on the new DORA regulation which is due to be in place for 2024. This would be best mentioned in the Business Continuity Management module which is part of the Cyber Risk Specialist cluster. When interviewing new graduates, a lot do not have experience or even knowledge of new regulations. It could also be added as recommended reading/resource.

12. Quality assurance procedures

- Has evidence been provided of the application of TU Dublin quality assurance procedures in the development of the proposed programme?
- Has evidence been provided that procedures exist for the ongoing monitoring and periodic review of programmes?

12.1 Section 1.3 outlines clear statement in relation to academic management and programme monitoring.

12.2 The exists a programme monitoring process that allows regular consideration of course quality. It is the policy of the University that a programme monitoring report on the operation of each programme be maintained. This monitoring and evaluation activity, carried out by the course boards and the programme board, provides an objective basis for maintaining and enhancing the quality of the educational provision.

13. Review Panel Recommendations

13.1 The panel recommends that the programme be validated with Recommendations[1].

13.2 The programme team was commended for preparing quality documentation for assessment.

13.3 Salient Recommendation to be addressed in conjunction with the issues raised in Part 1 through Part 12 of this report:

(a) PO6 should be adequately addressed for the Postgraduate Diploma award.

[1] A recommendation is a proposed action, which in the opinion of the validation panel, must be given serious consideration.

(b) Programme team to consider reviewing the "Cyber Risk Specialist" option on the Postgraduate Certificate. The title suggests an emphasis on risk management, but none of the modules are focused on risk management. Each of them as an element of risk, but given the title of the option, one would expect a module focused on risk management. The other two options have modules that relate directly to the title, but the "Cyber Risk Specialist" doesn't have that.

(c) The Secure Programming module should be reconsidered. Without a background in software development, it could be hard for students to grasp the concepts of writing secure code. The panel noted that even experienced Security Professionals struggle with this.

(d) There are some topics not covered, but which are important and need further consideration. For example, Vulnerability Management and Access Control are critical for any organisation to implement and are part of most security industry standards such as ISO 27001, CIS and NIST.

(e) The panel recommends addition of the following elements for programme enhancement, particularly, awareness of graduates of the programmes:

- Adding information on Security Frameworks (e.g., NIST, ISO, GDPR) as part of recommended resources if not covered in modules. It was noted that NIST is mentioned as a recommended resource, however, this is for the Biometrics module which is not part of the 3 proposed clusters.
- Incorporate new regulations into relevant areas. For example, clients are constantly asking questions on the new DORA regulation which is due to be in place for 2024. This would be best mentioned in the Business Continuity Management module which is part of the Cyber Risk Specialist cluster. When interviewing new graduates, a lot do not have experience or even knowledge of new regulations. It could also be added as recommended reading/resource.

Panel Secretary

_____ _____

Dr Philip Owende Date
Assistant Head of Academic Affairs

Response to Panel Recommendations

The panel recommends that the programme be validated with Recommendations.

The School team wishes to thank the Review Panel for their time and efforts in the consideration of these proposed programmes and welcomes their approval for validation.

Salient Recommendation to be addressed in conjunction with the issues raised in Part 1 through Part 12 of this report:

1. PO6 should be adequately addressed for the Postgraduate Diploma award.

   This was raised in section 8.2. There was a small number of missed mappings of module learning outcomes to the programme learning outcomes that has now been fixed. PO6 is about student reflecting on their strengths and weaknesses, and this is reflected in many modules where the students carry out research for knowledge of a topic and learning new processes, techniques and skills. There are five out of the eight elective modules that now have this learning outcome mapped correctly.

2. Programme team to consider reviewing the "Cyber Risk Specialist" option on the Postgraduate Certificate. The title suggests an emphasis on risk management, but none of the modules are focused on risk management. Each of them as an element of risk, but given the title of the option, one would expect a module focused on risk management. The other two options have modules that relate directly to the title, but the "Cyber Risk Specialist" doesn't have that.

   This was raised in section 3.4 and 8.3. Cyber Security is about risk identification and risk management, so this is a theme in Security Intelligence, Application Security and Business Continuity Management. Each module address risk from a different point of view, Security intelligence looks at the risk of cyber-attacks before they happen, Business Continuity is mitigating the business risk and Application Security for mitigating the technical risk.

3. The Secure Programming module should be reconsidered. Without a background in software development, it could be hard for students to grasp the concepts of writing secure code. The panel noted that even experienced Security Professionals struggle with this.

   This was raised in section 6.4 and 8.4. Candidates for entry to this course will have a background in computing and as such, should have the fundamentals of programming. The Secure Programming module builds on the fundamentals of programming by looking at the software development architecture and processes and explores how secure coding techniques can mitigate against popular cyber-attacks. This module is not about training Security Professionals to be programmers but instead to instil in programmers' security awareness and to implement good coding processes to reduce the vulnerabilities in applications.

4. There are some topics not covered, but which are important and need further consideration. For example, Vulnerability Management and Access Control are critical for any organisation to implement and are part of most security industry standards such as ISO 27001, CIS and NIST.

   This was raised in section 8.5. The PG-Cert programmes are groupings of three modules that target particular roles within industry so would not be able to cover a broad range of modules which is why we have the PG-Diploma that covers a much broader range of topics within cybersecurity. Vulnerability management, Access Control and Industry Standards are subtopics and are addressed in every module

to some extent and more so, in other modules such as Business Continuity Management, Secure Communications, Network Security, Secure Programming, and Biometrics.

5. The panel recommends addition of the following elements for programme enhancement, particularly, awareness of graduates of the programmes:
    a. Adding information on Security Frameworks (e.g., NIST, ISO, GDPR) as part of recommended resources if not covered in modules. It was noted that NIST is mentioned as a recommended resource, however, this is for the Biometrics module which is not part of the 3 proposed clusters.
    b. Incorporate new regulations into relevant areas. For example, clients are constantly asking questions on the new DORA regulation which is due to be in place for 2024. This would be best mentioned in the Business Continuity Management module which is part of the Cyber Risk Specialist cluster. When interviewing new graduates, a lot do not have experience or even knowledge of new regulations. It could also be added as recommended reading/resource.

    This was raised in Resources section 11.3. Both of these points are noted and will be taken in consideration within the delivery of the content of each module. Content for modules is indicative and is constantly reviewed and updated to keep abreast of the changes in standards, frameworks and improvement in technology.

6. Answers to other issues raised in Parts 1 to 12 were:
    a. Section 5.2 asked about the delivery of programmes: Programmes will be available for delivery in full-time, part-time and hybrid modes to address the flexibility of programme delivery for industry.
    b. Section 6.3 asked about RPL/WDL processes: This is part of the access process and marketing of these courses will include links to University policies on access requirements.
    c. Section 7.2 and 7.3 asked about the Research Skills bridging module: This module is a SPA of 10 credits if taken in isolation but for the 60-credit research project, it is integrated in the module as a series of workshops as the research project covers two semesters of work.