Independent Panel Report on a Provider's Programme Review

Provider	Dublin Business School ("DBS")
Programme(s) Reviewed	**Principal Programme:** Master of Science in Cybersecurity **Embedded Programme (Exit-only Award):** Postgraduate Diploma in Science in Cybersecurity

Independent Panel Members

Name	Role on Panel	Affiliation
Dr Annie Doona	Chair	Education Consultant and Former President, IADT
Matthew Hurley	Report Writer	Independent Consultant
Dr Anila Mjeda	Academic	Lecturer in Cybersecurity, Munster Technological University
Renaat Verbruggen	Academic	Assistant Professor, Dublin City University
Tom Chothia	Academic (International)	Professor of Cybersecurity, University of Birmingham
Howard Shortt	Industry Representative	Director of Cyber and Forensics, PwC Ireland
Damien Doherty	Learner Representative	NStEP Trained in Quality Assurance

All members of the independent panel declared their independence of Dublin Business School and that they have no conflict of interest

Part 1. Introduction

In accordance with statutory requirements and DBS internal review and revalidation process, an external, independent Panel convened on 21 January 2025 to conduct an evaluation of DBS' MSc in Cybersecurity programme and the embedded, exit-only Postgraduate Diploma in Science in Cybersecurity, for which DBS has sought revalidation.

Part 2. Evaluation Process

2.1 Documents Supplied to the Panel

	Document Type	**Document Name**
1.	CVs	Programme Team CVs
2.	Descriptor	Module and Assessment Document
3.	Descriptor	Programme Document
4.	Guidebook	Postgraduate Dissertation Guidebook
5.	Handbook	MSc in Cybersecurity Programme Handbook
6.	Regulatory Requirements	• DBS Cover Letter Declaration • Deed of Guarantee • Fee Cover Note • PEL Refund Arrangements
7.	Report	Programme Review Report
8.	Supporting Documents	• 2020 Validation Documents • Board of Studies reports • Certificates of Validation • Enrolment, Progression and Graduate Data • Exam Papers (CA Samples) • External Examiner Report • Independent Evaluation Report • Learner, Alumni and Industry Feedback • Programme Reports • QQI Criteria • Postgraduate Applied Research Project Guidebook • Postgraduate Business Guidebook • Research, Innovation, Practice, Enterprise Strategy • DBS Slate2 2023
9.	Terms of Reference	MSc in Cybersecurity Programme Review

2.2 Provider's Representatives Met

	Person	Role / Job Title
1.	Lori Johnston	Academic Dean
2.	David Williams	Academic Director
3.	Paul McEvoy	Assistant Academic Director / Programme Level Manager, MSc in Cybersecurity / Lecturer
4.	Andrew Browne	Dissertation Coordinator
5.	Shane Mooney	Head of Student Experience
6.	Darragh Breathnach	Registrar & Director of Campus Operations
7.	Anita Dwyer	Assistant Registrar
8.	Emma Balfe	Head of Teaching Delivery and Content Production
9.	Amy Hayes	Programmes Manager
10.	Sarah Sharkey	Student Engagement Officer
11.	Marina Nunes	Reader Services Manager
12.	Francisca Knight	Head of Academic Operations
13.	Nicholas Kelly	Faculty Manager
14.	Tamires Secco	Programme Coordinator
15.	Trevor Haugh	Head of Academic Information & Resource Centre
16.	Pete Cassidy	Lecturer
17.	Mina Ghazremanzamaneh	Lecturer
18.	Tejas Bhat	Lecturer
19.	Luciana Nascimento	Lecturer
20.	Swati Dongre	Lecturer
21.	Kingsley Ibomo	Lecturer
22.	6x Student Representatives	n/a

2.3 Description of evaluation process

Upon receipt of the programme documentation, members of the independent Panel conducted an initial desk review and provided written commentary highlighting areas where clarification or further probing may be needed.

The Panel had an opportunity to meet privately prior to the virtual site visit, which allowed for discussion about the programme review process, the revised programme, its modules and module assessments, and the quality assurance arrangements underpinning the programme. From this discussion, the Panel was able to identify specific areas of questioning during the virtual site visit, which took place on 21 January 2025.

During the site visit, the Panel met with DBS representatives at all levels, including senior management, programme-level managers, module leads, lecturers, and administrative and support staff. The Panel also met with a number of learner representatives and graduates who offered valuable insight into the learner experience.

Overall, the Panel found that the programme was well-developed, with strong demand and increasing application numbers. Consequently, at the conclusion of the virtual site visit, the Panel had no significant concerns in relation to the programme, although a number of recommendations were identified for DBS' consideration. Notwithstanding this, the Panel is pleased to make a recommendation that the programme is satisfactory.

Part 3. Panel Findings on Provider Programme Review Report

The following is the panel's commentary and recommendations on the provider's programme review report. It follows the section structure of the report in headings and in sequence. References to specific parts of the provider report will use the relevant report reference e.g. 2.2.4 Programme Management

Section A. Context and Terms of Reference for the Programme Review

Commentary:

QQI's Programme Review Manual (2022) states that "The objectives of a programme review are to evaluate the programme as implemented in light of the provider's experience of providing the programme over the previous five years..." (p. 5), with a view to making a number of determinations as to the programme's evolution, effectiveness, continued viability, relevance, currency, and alignment with regulatory guidelines and industry expectations.

In accordance with these statutory requirements and DBS' own programme review process, the following principal programme and embedded exit-only award have been put forward for revalidation:

- **Principal Programme**: The Level 9, 90 ECTS Master of Science in Cybersecurity
- **Embedded Programme (Exit-only award):** The Level 9, 60 ECTS Postgraduate Diploma in Science in Cybersecurity

Recommendations:

The Panel is satisfied with the context and terms of reference for the programme review and has no specific recommendations to make.

Section B. Provider Information and Programme Context

Commentary:

Founded in 1975, DBS is a Dublin City-based higher education institution offering programmes from levels 6 to 9 on the National Framework of Qualifications (NFQ). These programmes span a range of disciplines, including accounting, business, film and creative media, finance, humanities and social sciences, law, marketing and the computer sciences.

A subsidiary of Kaplan Inc., DBS has an active base of over 8,000 learners in addition 466 members of staff, comprised of 306 academic staff and 157 administrative staff.

The MSc in Cybersecurity is positioned within DBS' Computing Discipline, one of six disciplines overseen by the Academic Director, and aims to provide "theoretical knowledge and advanced skills in technology, communication information management and related processes that will enable assured business operations in the context of threat identification and mitigation" (Programme Review report, Section 2.3.1, p. 30).

Recommendations:

The Panel is satisfied with the provider information and programme context provided and has no specific recommendations to make.

Section C. Baseline qualitative and quantitative information

Programme Data Overview

Commentary:

Over the last validation period, application numbers have seen a significant year-on-year increase, from 164 in the 2020/21 academic year to 1,237 in the 2023/24 academic year. This indicates not only demand for the programme but the growing relevance of cybersecurity as a discipline and the need for cybersecurity professionals.

While enrolment numbers have increased year-on-year also, this has been a more measured growth: 12 out of 164 applicants in 2020/21, 73 out of 430 applicants in 2021/22, and 119 out of 837 applicants in 2022/23. A notably higher conversion rate of 18% in 2021/22 (compared to 7% in 2020/21 and 14% in 2022/23) has been attributed to an "influx of enrolments due to the changing socioeconomic landscape as a result of the pandemic" (PRR, Section 3.1.2.2, p. 37).

There is a notable gender disparity among enrolled learners, though this has lessened year on year, from a 100% male cohort in 2020/21 to 77.60% male / 22.40% females in 2023/24. DBS acknowledges this imbalance, highlighting it as an example of a broader trend within STEM education. The Panel recognises that as an issue that exists beyond DBS but recommends nonetheless that DBS give consideration to how it can improve the gender balance on the programme, in relation to both learners and staff.

Along with the increase in enrolment numbers over the last validation period, DBS recorded a decline in exam participation and pass rates, in addition to higher failure, withdrawal, and non-activity rates. The 2022/23 academic year was of particular note, with only 59.52% of learners in one of the year's three cohorts (approx. 20 out of 40 students, given that there are 119 students across all three cohorts) sitting for exams. DBS cited a number of factors influencing this, mostly relating to financial and cost-of-living concerns.

Recommendations:

- Considering DBS' strategic intent to increase enrolment numbers over the next validation period, the Panel recommends that DBS closely monitor its capacity and resource availability (physical and human) to ensure these remain viable.

- The Panel recommends that DBS give further consideration to how it can improve the gender balance on the programme, in relation to staff and students.

Programme Delivery and Teaching & Learning Strategies

Commentary:

The Programme Review Report notes DBS' considerable investment in recent years to enhance its physical, ICT and learner support service environments. The learning environment includes access to a physical library (open 6 days a week) and online library (available 24/7), Moodle VLE access, Zoom and BigBlueButton access, a dedicated Media Lab, WiFi, classrooms with interactive whiteboards, overhead projectors and other A/V equipment used in multimedia delivery, computer labs, an OpenStack environment for utilising web servers, FTP servers, SQL servers and Linux, and IT supports.

Attendance data over three academic years (2020/21, 2021/22, and 2022/23) exhibited sizable fluctuations, with the 2022/23 year recording the lowest average attendance. Despite DBS' view of satisfactory attendance being 85% or above, attendance rates in 202/23 were below 75% across all modules, with one module seeing a decline to 48.73%. DBS has acknowledged this as an emerging challenge concerning learner engagement and has committed to implement more "proactive monitoring for early signs of disengagement and cross-departmental collaborations to provide comprehensive student support and cultivate a more engaging learning environment" (Programme Review Report, Section 3.2.4.2, p. 63).

Extending from the above, DBS has slightly revised the staff to learner ratios for different learning activities to allow for better monitoring of learner engagement and performance. While classroom sessions will remain at 1:60, practical sessions and workshops will be set at 1:30, as will live online classes.

DBS endeavours to employ a number of teaching and learning strategies on the programme, including active learning, real-world application, guest speakers and workshops, and continuous feedback. In its review and revision of the programme, a renewed focus was placed on practical skills development to ensure the curriculum is aligned with the needs of industry and that learners leave the programme equipped with work-ready skills. However, the review also found the provision of formative feedback to learners to be inconsistent, with learners reporting issues with the timeliness and depth of feedback.

The review of the programme aimed to ensure the assessment strategy was constructively aligned with the learning outcomes and provided a means for the programme team to incorporate more practical assessment types to "directly evaluate students' abilities to apply their knowledge and skills in practical settings" (Programme Review Report, Section 3.2.7.1, p. 72). The decision was also made to remove exams entirely from the programme in order to place a greater emphasis on portfolio-based assessments so that graduates could showcase their work and abilities to prospective employers.

Recommendations:

- The Panel recommends that DBS review its approach to assessment feedback to ensure:
    - Feedback is more consistently delivered within a reasonable timeframe.
    - Feedback is provided at more frequent intervals during a module.

    - The timing and depth of feedback is sufficient to help learners identify areas of strength and areas requiring further enhancement.

- The Panel recommends that DBS reflect on its decision to entirely remove exams from the programme, considering whether there may be instances in which exams could prove useful, as in module assessments where there is otherwise a risk of plagiarism.

Section D. Evaluation of the programme by stakeholders

Evaluation by current learners and graduates of the programme

Commentary:

In order to gather learner and graduate perspectives on the programme, DBS prepared two surveys, one for each cohort. 40 respondents, 6 alumni and 34 current learners, provided feedback on a range of factors including whether the programme and its modules met their expectations, skill-development opportunities available and missing, the mode of delivery, the workload, the assessment strategy, and DBS' facilities, among others.

The provision of timely and constructive feedback was a recurring issue raised by learners and graduates, with some noting that feedback was only provided at the end of a module or summative assessment, meaning there was no opportunity to integrate the feedback into their learning practice ahead of a subsequent assessment.

Learners also noted a desire for more practical, hands-on experience which DBS aims to address by ensuring the alignment of the programme with industry needs and by "integrating tool usage into existing modules" (Programme Review Report, Section 4.1.3, p. 88).

Recommendations:

- The Panel recommends that DBS review its approach to assessment feedback to ensure:
    - Feedback is more consistently delivered within a reasonable timeframe.
    - Feedback is provided at more frequent intervals during a module.
    - The timing and depth of feedback is sufficient to help learners identify areas of strength and areas requiring further enhancement.

Evaluation of the programme by Staff

Commentary:

Feedback from the programme team indicated that while faculty are overall satisfied with the programme, certain changes such as an increased focus on academic scholarship and a move away from traditional exams have been proposed for the revised programme "to ensure a smoother learning experience" (Programme Review Report, Section 4.2.3, p. 90). Accordingly, the programme team has opted to include a new 5-credit Research Methods module in Semester 1 to complement the 5-credit Applied Research Methods module in Semester 2. Further, DBS has moved toward a portfolio-based system of assessment intended to allow "learners to showcase a broader range of skills and abilities" (Programme Review Report, Section 4.2.3, p. 90).

Recommendations:

- The Panel recommends that DBS reconsider its decision to include two modules on research methods given the mostly practical, skills-based focus of the programme. This is in light of the fact that the programme is skills-based with a largely practical focus, and therefore one instead of two research-based modules may be sufficient.
- The Panel recommends that DBS reflect on its decision to entirely remove exams from the programme, considering whether there may be instances in which exams could prove useful, as in module assessments where there is otherwise a risk of plagiarism.

External Examiner Feedback

Commentary:

External examination for the programme has been conducted systematically and in line with defined procedures, providing the programme team with independent oversight of its assessment practices. Feedback from External Examiners has been overall positive; nonetheless there have been a number of recommendations to provide comprehensive rubrics to enhance the transparency and fairness of assessments, the subsequent implementation of which appeared to address the issue.

External Examiner feedback also highlighted the challenges relating to plagiarism and generative AI, addressing which is likely to involve "redesigning assessments to focus on higher-order thinking skills, and education students about academic integrity and responsible AI use" (Programme Review Report, Section 4.3.3, p. 97)

Recommendations:

The Panel has no specific recommendations to make.

Section E. Programme Quality Assurance

Complaints, appeals and commendations

Commentary:

From the Programme Review Report alone, the Panel was unable to discern whether the programme had seen any complaints or appeals over the last validation period, and if so, how many. This was due to a focus in the report on policy rather than data. This was queried with DBS representatives during the site visit who acknowledged the omission and subsequently provided the Panel with a spreadsheet of data regarding complaints and appeals for the programme over the last five years.

While there were no particular concerns for the Panel within the presented data, and any arising matters appeared to be addressed in line with established policy, the Panel advised DBS to include details of these figures as standard practice in its future programme review reports.

Recommendations:

- The Panel recommends that DBS include details about the number of complaints and appeals received over the last validation period within the Programme Review Report, and indicate whether these were resolved in accordance with defined procedures, even if this number is zero.

Quality Assurance Systems and Processes

Commentary:

DBS has a well-established quality assurance system underpinning the development and delivery of its programmes and this is subject to ongoing review and revision as required. The Panel is satisfied that the programme has been internally reviewed in accordance with DBS' internal processes and welcomes the ongoing efforts of DBS to continue its training and information sessions for faculty.

Recommendations:

The Panel has no specific recommendations to make.

Additional Quality Assurance Systems and Processes required (e.g. online delivery / assessment)

Commentary:

The programme does not require any additional quality assurance processes that are not already covered by DBS' overarching quality assurance system. Where such a need arises, the Panel is satisfied that DBS has the capacity and expertise to develop and implement these.

Recommendations:

The Panel has no specific recommendations to make.

Section F. Summary Analysis of the programme

Commentary:

As part of its programme review process, DBS conducted a SWOT analysis which highlighted the strength of the curriculum, the programme's practical, hands-on focus, its responsiveness to industry needs, and its success rate in producing work-ready graduates. In contrast, the notable gender imbalance was acknowledged, as were the issues around the provision of feedback to learners and the need to further enhance the programme's assessment strategy.

The increasing industry demand for cybersecurity professionals and the programme's ability to integrate emerging technologies were identified as opportunities, while the industry's rapid evolution and competition from other providers offering similar programmes have been cited as threats.

Recommendations:

The Panel is satisfied that the analysis of the programme reflects genuine consideration of the programme's strengths, weaknesses, opportunities and threats. No specific recommendations have been identified.

Section G. Revision of the programme

Commentary:

DBS has proposed the following revisions to the programme:

1. DBS is proposing to increase the maximum enrolment from 150 learners per year to 600 per year; up to 120 per intake.

2. DBS is proposing to add a 'Research Methods' module and an elective 'Dissertation' module to the programme.

3. DBS is proposing to change the 'Applied Research Project' to an elective (to coincide with the introduction of the new 'Dissertation' module, which learners will have a choice between.

4. DBS is proposing to reduce the number of credits allocated to the 'Advanced Programming Techniques' module from 10 to 5.

5. DBS has proposed a number of changes to its teaching and learning strategy, including a move toward more online delivery.

6. DBS has proposed a number of changes to its assessment strategy, including the removal of proctored exams and the (re-)introduction of practical demonstrations as part of continuous assessments.

Recommendations:

The Panel is satisfied that, on the whole, the proposed revisions to the programme are relevant and appropriate, with a supporting rationale that has been informed by stakeholder feedback. Notwithstanding this, some recommendations have been identified for DBS' consideration, noted in Part 4, Section D below, and in the Independent Evaluation Report.

Part 4. Overall Findings

In this section the panel will give its overall feedback on the conduct of the review and the findings therein. This feedback will inform future provider review processes and will also contribute to the refinement of any programmes being proposed for revalidation following this review process.

Section A. Commentary on review process:

The Panel is satisfied that the programme review process was conducted in accordance with established processes and with a view to genuine enhancement of the programme, and was appropriately informed by a broad range of stakeholders to ensure alignment with both learner and industry needs.

Section B. Recommendations on review process:

For clarity and transparency in future review reports, the Panel recommends that DBS review its use of language in the Programme Review Report to ensure it is clear whether an action has been implemented and to what extent, and that DBS includes details about the number of complaints and appeals received over the last validation period within the Programme Review Report, and whether these were resolved in accordance with defined procedures, even if this number is zero.

Section C. Commentary on programme revisions:

The Panel is satisfied that, on the whole, the proposed programme revisions represented warranted changes informed by feedback from learners, graduates, staff, external stakeholders, and external examiners. Notwithstanding this, the Panel advises DBS to reflect on and reconsider some of its decisions, given their implications. These pertain to areas such as the decision to include two modules on research methods given the otherwise skills-based focus of the programme, and the decision to remove exams entirely from assessments.

Section D. Recommendations on programme revisions:

The Panel has identified thirteen recommendations for DBS' consideration:

1. The Panel recommends that DBS consider offering elective modules to meet the needs of learners with different career ambitions.

2. The Panel recommends that DBS reconsider its decision to include two modules on research methods given the mostly practical, skills-based focus of the programme.

3. In relation to the Advanced Programming Techniques module, the Panel recommends:
    a. that DBS reconsider the use of the word 'Advanced' in the title.
    b. that DBS more visibly cover secure software in the module content.
    c. that DBS review the current group assessment worth 70% of the overall grade to ensure that this is an authentic assessment.

4. The Panel recommends that DBS consider the inclusion of additional modules around cybersecurity.

5. The Panel recommends that DBS more clearly articulates the coverage of operational technology standards, policy and risk analysis within the indicative module content.

6. The Panel recommends that DBS incorporates the most recent EU legislation and regulations on cybersecurity within the programme.

7. The Panel recommends that DBS review its approach to assessment feedback to ensure:

    a. Feedback is more consistently delivered within a reasonable timeframe.
    b. Feedback is provided at more frequent intervals during a module.
    c. The timing and depth of feedback is sufficient to help learners identify areas of strength and areas requiring further enhancement.

8. The Panel recommends that DBS reflect on its decision to entirely remove exams from the programme.

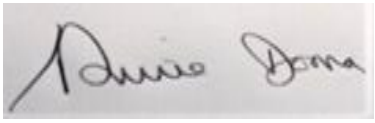
9. The Panel recommends that DBS consider developing and instituting guidelines for faculty on how to teach and assess in the age of generative AI (which may complement the existing learner-facing guidelines on gen AI use).

10. Considering DBS' strategic intent to increase enrolment numbers over the next validation period, the Panel recommends that DBS closely monitor its capacity and resource availability (physical and human) to ensure these remain viable.

11. The Panel recommends that DBS give further consideration to how it can improve the gender balance on the programme, in relation to staff and students.

12. The Panel recommends that DBS include details about the number of complaints and appeals received over the last validation period within the Programme Review Report, and indicate whether these were resolved in accordance with defined procedures, even if this number is zero.

13. The Panel recommends that DBS review its use of language in the Programme Review Report to ensure it is clear whether an action has been implemented and to what extent.

Signed: ___  __Dr Annie Doona_____
Panel Chairperson:

Date: ____21st March 2025_____

Dearbhú Cáilíochta
agus Cáilíochtaí Éireann
Quality and
Qualifications Ireland

Independent Evaluation Report on an Application for Revalidation of a Programme of Education and Training

Part 1. Provider details

Provider name	Dublin Business School ("DBS")
Date of site visit	21 January 2025
Date of report	31 January 2025

Section A. Overall recommendations

Principal programme[1]	**Title**	Master of Science in Cybersecurity
	Award	Master of Science (Major Award)
	Credit	90
	Recommendation *Satisfactory OR Satisfactory subject to proposed conditions OR Not Satisfactory*	Satisfactory

Embedded programme 1[2]	**Title**	Postgraduate Diploma in Science in Cybersecurity
	Award	Postgraduate Diploma in Science (Major Award)
	Credit	60
	Recommendation *Satisfactory OR Satisfactory subject to proposed conditions OR Not Satisfactory*	Satisfactory

[1] Replace throughout with actual programme title.
[2] Replace throughout with actual programme title. Copy and paste this table for any additional embedded programmes.

Section B. Expert Panel

Name	Role	Affiliation
Dr Annie Doona	Chair	Education Consultant and Former President, IADT
Matthew Hurley	Report Writer	Independent Consultant
Dr Anila Mjeda	Academic	Lecturer in Cybersecurity, Munster Technological University
Renaat Verbruggen	Academic	Assistant Professor, Dublin City University
Dr Tom Chothia	Academic (International)	Professor of Cybersecurity, University of Birmingham
Howard Shortt	Industry Representative	Director of Cyber and Forensics, PwC Ireland
Damien Doherty	Learner Representative	NStEP Trained in Quality Assurance

Section C. Principal Programme: Master of Science in Cybersecurity

Names of centre(s) where the programme(s) is to be provided	Maximum number of learners *(FT)*	Maximum number of learners *(PT)*
Dublin Business School, 13-14 Aungier Street, Dublin 2	360	240

Proposed Duration and Enrolment					
	First Intake Date	Duration	Intakes per Annum	Enrolment i.e. learners per Intake	
			Maximum	Minimum	Maximum
Full-Time	Sept 2025	1 Year / 12 Months	3	10	120
Part-Time	Sept 2025	2 Years / 24 months	2	10	120
Intake Schedule e.g. January September		September, January, March/April			

Panel Commentary on proposed enrolment:

Considering DBS' strategic intent to increase enrolment numbers over the next validation period, the Panel recommends that DBS closely monitor its capacity and resource availability (physical and human) to ensure these remain viable.

Brief synopsis of the programme (e.g. who it is for, what is it for, what is involved for learners, what it leads to.)

"The Masters programme is designed to meet the growing need for Cybersecurity provisions throughout the workforce. Underlying this emergence is the need to prepare specialists across a range of work roles for the complexities associated with assuring the security of system operations from a holistic view."

"The Master of Science in Cybersecurity programme is aimed at developing learners within the cybersecurity discipline and provides theoretical knowledge and advanced skills in technology, communication information management, and related processes that will enable assured business operations in the context of threat identification and mitigation. The cybersecurity discipline involves a broad range of technological needs including the creation, operation, analysis, and testing of secure computer systems. The programme also recognises the interdisciplinary nature of cybersecurity, and incorporates learning on law, policy, human factors, ethics, and risk management."

"The programme has been designed to meet the growing need for cybersecurity provisions throughout the workforce. Given society's increasing dependence on the global cyber infrastructure, cybersecurity is now emerging as a distinct knowledge area. It has become an identifiable discipline with a breadth and depth of content that encompasses many of the subfields (e.g. software development, networking, database management) to form the modern computing ecosystem. Underlying this emergence is the need to prepare specialists across a range of work roles for the complexities associated with assuring the security of system operations from a holistic view. Business objectives now require effectively managing risk, done by constantly monitoring, assessing, and responding to cyber threats directed towards businesses and development/implementation of mitigating controls."

"This programme aims at developing learners within the Cybersecurity discipline and involves theoretical knowledge and advanced skills in technology, communication information management, and processes, to enable assured operations in the context of threat identification and mitigation."

"The current generation of cyberattacks differ from their predecessors in a variety of ways, the most prevalent difference being the wide range of technologies that they can target, from mobile phones to entire cloud networks. As a result, attacks can occur across countries, companies, and even continents. This programme aims to fill the ever-increasing skills gap in this area and delivers material that follows the most current practice."

"Learners initially develop advanced practical skills in essential areas such as programming, advanced databases, networks and systems administration, while also acquiring theoretical knowledge of cryptography and digital forensics. Furthering the learner's abilities in cybersecurity the programme offers applied skills in contemporary topics such as software development, communications and networking security, and organisational and societal cybersecurity."

"The programme also incorporates professional development within the learning of each module in order to support learners in enhancing their employability options. This will enable the learner to integrate seamlessly into an organisation by addressing skills such as awareness of social media, leadership, self-management, teamwork, research skills, and advanced academic writing and critical abilities that are essential for a Level 9 graduate. The Master of Science programme also comprises an Applied Research Methods module, which focuses on research and development skills. This module will inform the learner's choice of an Applied Research Project for those who complete the Master's programme."

[Extracted from Programme Descriptor, Section 1C.1.12, pp. 19-20]

Target learner groups

" The Master of Science in Cybersecurity programme is aimed at learners with a minimum-second-class second-division (2.2) Level 8 honours bachelor's degree or Higher Diploma in a cognate area who wish to specialise in the field of cybersecurity with a view to entering industry. Cognate

subjects include computer science, technology, networking, information systems, engineering, general science, mathematics, statistics, data analytics, or related disciplines."

"The programme has specific aims to cultivate a deep understanding of current and emerging computer technologies, particularly in the development and use of cybersecurity systems. It also provides students with the knowledge and skills to effectively manage cybersecurity systems within organisational contexts."

"Recognising the dynamic nature of the computing sector, the programme promotes the development of autonomous learning skills, enabling graduates to adapt to evolving industry needs. It also instills a strong ethical awareness, preparing graduates to respond thoughtfully to unforeseen challenges."

"Ultimately, this programme provides a comprehensive foundation for career development, innovation, and further study in the field of cybersecurity. Graduates will possess a critical understanding of core concepts, enhanced practical skills, and the research capabilities needed to excel in this dynamic field.

[Extracted from Programme Descriptor, Section 1C.1.13, p. 21]

Approved countries for provision	Ireland
Delivery mode: Full-time/Part-time	Full-time and Part-time

The teaching and learning modalities
• On-site, face-to-face • Synchronous online • Asynchronous • Independent

Summary of specifications for teaching staff		
Role	**Profile**	**WTE**
Lecturer	Lecturing staff will have a minimum of a Master's and/or PhD in the following areas: • Computing Science / Computing • Quantitative Methods • Cybersecurity • Networking • Information Systems • Computer Technology • Research Methods • Mathematics and Statistics	10

Learning Activity	Ratio of learners to teaching staff
Classroom Sessions	1:60
Online Class (live)	1:30
Workshops	1:30
Practical Sessions	1:30

Panel Commentary on programme outline and staffing:

The Panel is satisfied that the programme outline and staff are appropriate in view of DBS' vision and intent for the programme.

Programmes being replaced (applicable to applications for revalidation)		
Code	**Title**	**Last enrolment date**
PG24326	Master of Science in Cybersecurity	December 2025

Section C2. Embedded Programme: Postgraduate Diploma in Science in Cybersecurity

Names of centre(s) where the programme(s) is to be provided	**Maximum number of learners** *(FT)*	**Maximum number of learners** *(PT)*
Dublin Business School, 13-14 Aungier Street, Dublin 2	N/A	N/A

Proposed Duration and Enrolment					
	First Intake Date	**Duration**	**Intakes per Annum**	**Enrolment i.e. learners per Intake**	
			Maximum	**Minimum**	**Maximum**
Full-Time	N/A	N/A	N/A	N/A	N/A
Part-Time	N/A	N/A	N/A	N/A	N/A
Intake Schedule e.g. January September		N/A			

Panel Commentary on proposed enrolment:

The Postgraduate Diploma is an exit-only award with no direct recruitment.

Brief synopsis of the programme (e.g. who it is for, what is it for, what is involved for learners, what it leads to.)

"There is one embedded programme in the Master of Science in Cybersecurity, a Postgraduate Diploma in Science in Cybersecurity. The Postgraduate Diploma is offered as an exit award for learners who cannot complete the full Master's programme."

"The programme has been designed to meet the growing need for cybersecurity provisions throughout the workforce. Given society's increasing dependence on the global cyber infrastructure, cybersecurity is now emerging as a distinct knowledge area. It has become an identifiable discipline with a breadth and depth of content that encompasses many of the subfields (e.g. software development, networking, database management) to form the modern computing ecosystem. Underlying this emergence is the need to prepare specialists across a range of work roles for the complexities associated with assuring the security of system operations from a holistic view. Business objectives now require effectively managing risk, done by constantly monitoring, assessing, and responding to cyber threats directed towards businesses and development/implementation of mitigating controls."

"This programme aims at developing learners within the Cybersecurity discipline and involves theoretical knowledge and advanced skills in technology, communication information management, and processes to enable assured operations in the context of threat identification and mitigation."

"The current generation of cyberattacks differ from their predecessors in a variety of ways, the most prevalent difference being the wide range of technologies that they can target, from mobile phones to entire cloud networks. As a result, attacks can occur across countries, companies, and even continents. This programme aims to fill the ever-increasing skills gap in this area and delivers material that follows the most current practice."

"Learners initially develop advanced practical skills in essential areas such as programming, advanced databases, networks and systems administration, while also acquiring theoretical knowledge of cryptography and digital forensics. Furthering the learner's abilities in cybersecurity, the programme offers applied skills in contemporary topics such as software development, communications and networking security, and organisational and societal cybersecurity."

"The programme also incorporates professional development within the learning of each module in order to support learners in enhancing their employability options. This will enable the learner to integrate seamlessly into an organisation by addressing skills such as awareness of social media, leadership, self-management, teamwork, research skills and academic writing and critical abilities that are essential for a Level 9 graduate."

[Extracted from Programme Descriptor, Section 1C.2.8, pp. 23-24]

Target learner groups
" The Postgraduate Diploma is offerd as an exit award for learners who cannot complete the full Master's programme." [Extracted from Programme Descriptor, Section 1C.2.9, p. 24]

Approved countries for provision	N/A
Delivery mode: Full-time/Part-time	N/A

The teaching and learning modalities
• On-site, face-to-face • Synchronous online • Asynchronous • Independent

Summary of specifications for teaching staff		
Role	**Profile**	**WTE**
Lecturer	Lecturing staff will have a minimum of a Master's and/or PhD in the following areas: • Computing Science / Computing • Quantitative Methods • Cybersecurity • Networking • Information Systems • Computer Technology • Research Methods • Mathematics and Statistics	10

Learning Activity	Ratio of learners to teaching staff
Classroom Sessions	1:60
Online Class (live)	1:30
Workshops	1:30
Practical Sessions	1:30

Panel Commentary on programme outline and staffing:

The Panel is satisfied that the programme outline and staff are appropriate in view of DBS' vision and intent for the programme.

Programmes being replaced (applicable to applications for revalidation)		
Code	**Title**	**Last enrolment date**
PG24327	Postgraduate Diploma in Science in Cybersecurity	December 2025

Section D. Other noteworthy features of the application

The Panel would like to commend DBS on:

1. its constructive engagement with the Panel during the site visit.
2. the relevance and currency of the programme's curriculum.

Part 1A Evaluation of the Case for an Extension of the Approved Scope of Provision (where applicable).

Having examined appropriate QA / Governance procedures, comment on the case for extending the applicant's Approved Scope of Provision to enable provision of this programme. (Especially relevant for move to online delivery / assessment)

Not applicable.

Part 2. Evaluation against the validation criteria

Criterion 1. The provider is eligible to apply for validation of the programme

a) The provider meets the prerequisites (section 44(7) of the 2012 Act) to apply for validation of the programme. b) The application for validation is signed by the provider's chief executive (or equivalent) who confirms that the information provided is truthful and that all the applicable criteria have been addressed. c) The provider has declared that their programme complies with applicable statutory, regulatory and professional body requirements.		
Programme	**Satisfactory? (yes, no, partially)**	**Comment**
MSc in Cybersecurity	Yes	The Panel is satisfied that DBS meets the prerequisites to apply for validation of the programme and that the application for validation is in compliance with all applicable statutory and regulatory requirements.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 2. The programme objectives and outcomes are clear and consistent with the QQI awards sought

a) The programme aims and objectives are expressed plainly.
b) A QQI award is specified for those who complete the programme.
    (i) Where applicable, a QQI award is specified for each embedded programme.
c) There is a satisfactory rationale for the choice of QQI award(s).
d) The award title(s) is consistent with unit 3.1 of QQI's Policy and Criteria for Making Awards.
e) The award title(s) is otherwise legitimate for example it must comply with applicable statutory, regulatory and professional body requirements.
f) The programme title and any embedded programme titles are
    (i) Consistent with the title of the QQI award sought.
    (ii) Clear, accurate, succinct and fit for the purpose of informing prospective learners and other stakeholders.
g) For each programme and embedded programme
    (i) The minimum intended programme learning outcomes and any other educational or training objectives of the programme are explicitly specified.
    (ii) The minimum intended programme learning outcomes to qualify for the QQI award sought are consistent with the relevant QQI awards standards.
h) Where applicable, the minimum intended module learning outcomes are explicitly specified for each of the programme's modules.
i) Any QQI minor awards sought for those who complete the modules are specified, where applicable.
j) For each minor award specified, the minimum intended module learning outcomes to qualify for the award are consistent with relevant QQI minor awards standards.

Programme	**Satisfactory? (yes, no, partially)**	**Comment**
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. The core aim of the programme is to provide learners with "critical understanding of cybersecurity skills, while also enhancing the research capability and practical technical skills of learner" (Programme Descriptor, 1C.1.12, p. 21). An associated list of eight programme objectives aligning with this overarching aim are plainly expressed. The decision to apply the science stem and award standards is justified given the programme's focus on technological content, computing and information systems, and the Panel is satisfied that the award title is consistent with QQI's Policy and Criteria for Making Awards. Similarly, the programme title is consistent with other similar programmes and is clear for the purpose of informing prospective learners and other stakeholders. Ten minimum intended programme learning outcomes (MIPLOs) are documents and the Panel is satisfied that these are consistent with the relevant QQI award standards.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 3. The programme concept, implementation strategy, and its interpretation of QQI awards standards are well informed and soundly based (considering social, cultural, educational, professional and employment objectives)

a) The development of the programme and the intended programme learning outcomes has sought out and taken into account the views of stakeholders such as learners, graduates, teachers, lecturers, education and training institutions, employers, statutory bodies, regulatory bodies, the international scientific and academic communities, professional bodies and equivalent associations, trades unions, and social and community representatives.
b) The interpretation of awards standards has been adequately informed and researched; considering the programme aims and objectives and minimum intended programme (and, where applicable, modular) learning outcomes.
    (i) There is a satisfactory rationale for providing the programme.
    (ii) The proposed programme compares favourably with existing related (comparable) programmes in Ireland and beyond. Comparators should be as close as it is possible to find.
    (iii) There is support for the introduction of the programme (such as from employers, or professional, regulatory or statutory bodies).
    (iv) There is evidence of learner demand for the programme.
    (v) There is evidence of employment opportunities for graduates where relevant.
    (vi) The programme meets genuine education and training needs.
c) There are mechanisms to keep the programme updated in consultation with internal and external stakeholders.
d) Employers and practitioners in the cases of vocational and professional awards have been systematically involved in the programme design where the programme is vocationally or professionally oriented.
e) The programme satisfies any validation-related criteria attaching to the applicable awards standards and QQI awards specifications.

Programme	Satisfactory? (yes, no, partially)	Comment
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. The Panel is satisfied that DBS and the programme team have taken a comprehensive approach to the programme review, engaging with a range of stakeholders including learners, graduates, staff, and external stakeholders. The Programme Descriptor sets out a clear rationale for continued provision of the programme and a benchmarking exercise has been conducted to show DBS' offering relative to other similar offerings in Ireland and the UK. The significant rise in applicants and enrolments over the last validation period is a strong indicator of demand for the programme, and DBS hopes to grow these numbers further up to a maximum of 600 learners per year across all intakes on the full-time and part-time versions of the programme. Evidence of employment opportunities has been provided, with DBS noting that "At the time of writing, there are over 100 active vacancies for graduate and postgraduate employment opportunities on [Indeed], 117 Cybersecurity graduate jobs in Ireland on [Glassdoor], and over 2,604 cybersecurity jobs in Ireland on LinkedIn" (Programme Descriptor, Section 3.6, p. 44). Five available posts were

		provided as additional evidence within the Programme Descriptor.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 4. The programme's access, transfer and progression arrangements are satisfactory

a) The information about the programme as well as its procedures for access, transfer and progression are consistent with the procedures described in QQI's policy and criteria for access, transfer and progression in relation to learners for providers of further and higher education and training. Each of its programme-specific criteria is individually and explicitly satisfied.
b) Programme information for learners is provided in plain language. This details what the programme expects of learners and what learners can expect of the programme and that there are procedures to ensure its availability in a range of accessible formats.
c) If the programme leads to a higher education and training award and its duration is designed for native English speakers, then the level of proficiency in English language must be greater or equal to B2+ in the Common European Framework of Reference for Languages (CEFRL[3]) in order to enable learners to reach the required standard for the QQI award.
d) The programme specifies the learning (knowledge, skill and competence) that **target learners** are expected to have achieved before they are enrolled in the programme and any other assumptions about enrolled learners (programme participants).
e) The programme includes suitable procedures and criteria for the **recognition of prior learning** for the purposes of access and, where appropriate, for advanced entry to the programme and for exemptions.
f) The programme title (the title used to refer to the programme):-
    (i) Reflects the core *intended programme learning outcomes*, and is consistent with the standards and purposes of the QQI awards to which it leads, the award title(s) and their class(es).
    (ii) Is learner focused and meaningful to the learners;
    (iii) Has long-lasting significance.
g) The programme title is otherwise legitimate; for example, it must comply with applicable statutory, regulatory and professional body requirements.

Programme	**Satisfactory? (yes, no, partially)**	**Comment**
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. The entry arrangements for the programme are plainly expressed in the Programme Descriptor (Section 4). Learners are generally required to possess a Level 8 Bachelor's Degree in a cognate area, or a Level 8 Higher Diploma in a cognate area, or a Level 8 Bachelor's degree in a non-cognate area but with at least 4 years of professional experience in a related field. Learners should also be competent at coding in an object-oriented programming language (e.g. C++, C#, Java, or Python). Learners may also apply for entry through DBS' RPL process, which is documented in its institutional Quality Assurance Handbook. Learners whose first language is not English must demonstrate a minimum English Language proficiency of B2+ on the Common European Framework of Reference for Languages (CEFRL) through the submission of IELTS or Cambridge certification.

[3] http://www.coe.int/t/dg4/linguistic/Source/Framework_EN.pdf (accessed 26/09/2015)

		While transfer options are not available for the programme, some inward and outward progression options are documented, such as onto PhD programmes in UCD and DCU.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 5. The programme's written curriculum is well structured and fit-for-purpose

a) The programme is suitably structured and coherently oriented towards the achievement by learners of its intended programme learning outcomes. The programme (including any stages and modules) is integrated in all its dimensions.
b) In so far as it is feasible the programme provides choice to enrolled learners so that they may align their learning opportunities towards their individual educational and training needs.
c) Each module and stage is suitably structured and coherently oriented towards the achievement by learners of the intended *programme* learning outcomes.
d) The objectives and purposes of each of the programme's elements are clear to learners and to the provider's staff.
e) The programme is structured and scheduled realistically based on sound educational and training principles.
f) The curriculum is comprehensively and systematically documented.
g) The credit allocated to the programme is consistent with the difference between the entry standard and minimum intended programme learning outcomes.
h) The credit allocated to each module is consistent with the difference between the module entry standard and minimum intended module learning outcomes.
i) Elements such as practice placement and work-based phases are provided with the same rigour and attentiveness as other elements.
j) The programme duration (expressed in terms of time from initial enrolment to completion) and its fulltime equivalent contact time (expressed in hours) are consistent with the difference between the minimum entry standard and award standard and with the credit allocation.

Programme	**Satisfactory? (yes, no, partially)**	**Comment**
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. On the whole, the Panel found the programme's structure and curriculum well developed and coherently oriented towards the achievement of both programme and module learning outcomes. Of the programme's 12 modules, all taught modules are mandatory, with no elective options. The only elective options on the programme concern a learner's choice between doing an Applied Research Project (Module 11) or a Dissertation (Module 12). In contrast, three out of the five institutions against which DBS benchmarked its programme offer a number of electives. Given the variety of career ambitious with which learners can enter onto the programme, the Panel suggested that some elective options, perhaps around management, understanding logs, or scripting, may prove helpful to learners. In respect of this, the Panel makes the following recommendation: **Recommendation 1** The Panel recommends that DBS consider offering elective modules to meet the needs of learners with different career ambitions. --

		The programme's structure includes two research-based modules, namely Research Methods and Applied Research Methods. DBS staff noted that this is a departmental decision based on experience of past learners struggling with designing a questions, understanding an artefact, and conduct literature reviews in a single module. To address this, DBS made the decision to create two 5-credit modules, one in semester 1 and the other in semester 2, allowing learners more time and opportunity to absorb the information and build on their learning. The separation of these modules means that Research Methods in semester 1 can focus on teaching learners how to design their question and prepare their literature review, while Applied Research Methods will focus on the production of an artefact. While acknowledging the rationale behind DBS' decision to split the module, the Panel queried whether two modules on Research Methods was, in fact, completely necessary given the programme's otherwise practical focus. In respect of this, the Panel makes the following recommendation: **Recommendation 2** The Panel recommends that DBS reconsider its decision to include two modules on research methods given the mostly practical, skills-based focus of the programme. -- In relation to the Advanced Programming Techniques module, around which much discussion was held during the site visit, the Panel sought to understand DBS' rationale for using the word "Advanced" in the title in spite of the fact cybersecurity doesn't necessarily involve heavy programming (scripting, yes, but not so much programming) and the module content does not appear to cover advanced techniques such as a security testing. Representatives for DBS commented that while they might describe the module as "foundational" because it is the "most grounding" programming module on the programme, they recognise that someone at an earlier stage in their career may struggle with it. Separately, the Panel noted that one of the assessments for Advanced Programming Techniques is a group assignment worth 70% of the module grade. However, it was not completely clear to the Panel what the group is expected to produce as part of this assignment and how DBS ensures it is an authentic assessment. DBS staff noted that they make their expectations of learners clear from the outset and that the assessment has been designed such that learners are developing to industry standards and can incorporate their work into

		their CV for presentation to industry. While accepting the value of this, the Panel found some of this underarticulated in the documentation. In respect of the points raised above, the Panel makes the following recommendation: **Recommendation 3** In relation to the Advanced Programming Techniques module, the Panel recommends: a. that DBS reconsider the use of the word 'Advanced' in the title. b. that DBS more visibly cover secure software in the module content. c. that DBS review the current group assessment worth 70% of the overall grade to ensure that this is an authentic assessment. -- In considering the overall suite of modules, the Panel noted that the taught modules are split between cybersecurity and computer science, with a slightly greater lean toward cybersecurity with nearly 50 credits. while not suggesting that this is an inappropriate split, the Panel is of the view that additional modules focused on cybersecurity may help reinforce the core focus of the programme. In respect of the points raised above, the Panel makes the following recommendation: **Recommendation 4** The Panel recommends that DBS consider the inclusion of additional modules around cybersecurity. -- On evaluation of the module content, the Panel was unable to find much coverage of operational technology. DBS staff noted that various case studies are introduced (focusing on the recent HSE cyber-attack, for example) which would refer to operational technology in varying ways. However, the Panel replied noting that, with operational technology, there is a risk of exposure and threat to life, meaning that the standards, policy, and risk analysis used within the operational technology environment are a key consideration. Similarly, the Panel found that some of the most recent EU legislation and regulations on cybersecurity appeared to be omitted from modules, perhaps given their recency, and that the programme's currency would benefit from their inclusion. In respect of the points raised above, the Panel makes the following recommendations:

		Recommendation 5 The Panel recommends that DBS more clearly articulates the coverage of operational technology standards, policy and risk analysis within the indicative module content. **Recommendation 6** The Panel recommends that DBS incorporates the most recent EU legislation and regulations on cybersecurity within the programme.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 6. There are sufficient qualified and capable programme staff available to implement the programme as planned

a) The specification of the programme's staffing requirements (staff required as part of the programme and intrinsic to it) is precise, and rigorous and consistent with the programme and its defined purpose. The specifications include professional and educational qualifications, licences-to practise where applicable, experience and the staff/learner ratio requirements. See also criterion 12 c).
b) The programme has an identified complement of staff (or potential staff) who are available, qualified and capable to provide the specified programme in the context of their existing commitments.
c) The programme's complement of staff (or potential staff) (those who support learning including any employer-based personnel) are demonstrated to be competent to enable learners to achieve the intended programme learning outcomes and to assess learners' achievements as required.
d) There are arrangements for the performance of the programme's staff to be managed to ensure continuing capability to fulfil their roles and there are staff development opportunities.
e) There are arrangements for programme staff performance to be reviewed and there are mechanisms for encouraging development and for addressing underperformance.
f) Where the programme is to be provided by staff not already in post there are arrangements to ensure that the programme will not enrol learners unless a complement of staff meeting the specifications is in post.

Programme	Satisfactory? (yes, no, partially)	Comment
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. Summary profiles of relevant staff members (Lecturers, the Academic Director, the Assistant Academic Director, the Programme Level Manager, Faculty Managers, and Programme Coordinators) are provided in the Programme Descriptor, and the Panel is satisfied that these are consistent with sectoral standards. DBS has confirmed that all staff necessary for the ongoing provision and management of the programme are already in situ. DBS has QQI-approved quality assurance procedures in place addressing the recruitment, management and development of staff, and the Panel had an opportunity to meet with staff at all levels of the programme, including senior management, academic faculty, and administrative and support staff, providing additional assurance that staffing is managed with the necessary rigor and consistency. However, the Panel observed an apparent gender imbalance among the programme's faculty, despite DBS on the whole having a gender-balanced staff. This links to an improving but still notable gender imbalance among learners enrolling on the programme, which is discussed further under Criterion 12.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 7. There are sufficient physical resources to implement the programme as planned

a) The specification of the programme's physical resource requirements (physical resources required as part of the programme and intrinsic to it) is precise, and rigorous and consistent with the programme, its defined purpose and its resource/learner-ratio requirements. See also criterion 12 d).
b) The programme has an identified complement of supported physical resources (or potential supported physical resources) that are available in the context of existing commitments on these e.g. availability of:
   (i) suitable premises and accommodation for the learning and human needs (comfort, safety, health, wellbeing) of learners (this applies to all of the programme's learning environments including the workplace learning environment)
   (ii) suitable information technology and resources (including educational technology and any virtual learning environments provided)
   (iii) printed and electronic material (including software) for teaching, learning and assessment
   (iv) suitable specialist equipment (e.g. kitchen, laboratory, workshop, studio) – if applicable
   (v) technical support
   (vi) administrative support
   (vii) company placements/internships – if applicable
c) If versions of the programme are provided in parallel at more than one location each independently meets the location-sensitive validation criteria for each location (for example staffing, resources and the learning environment).
d) There is a five-year plan for the programme. It should address
   (i) Planned intake (first five years) and
   (ii) The total costs and income over the five years based on the planned intake.
e) The programme includes controls to ensure entitlement to use the property (including intellectual property, premises, materials and equipment) required.

Programme	**Satisfactory? (yes, no, partially)**	**Comment**
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. DBS has, at its disposal, 47 lecture rooms fitted with interactive whiteboards, overhead projectors and other A/V equipment used in multimedia deliver, over 20 computer and mobile labs across two buildings, a physical library which is open 6 days a week, an online library available 24/7, a virtual learning environment (VLE) (Moodle), a dedicated Media Lab, and an OpenStack environment for utilising web servers, FTP servers, SQL servers and Linux, and IT supports. IT support is facilitated through the Computer Services department, which provides supports for learners studying both on and off-campus. The Programme Descriptor includes a table of projected income and expenditure over the next five years based on the provision of part-time and full-time versions of the programme, multiple intakes per year, and a proposed increase in enrolments.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 8. The learning environment is consistent with the needs of the programme's learners

a) The programme's physical, social, cultural and intellectual environment (recognising that the environment may, for example, be partly virtual or involve the workplace) including resources and support systems are consistent with the intended programme learning outcomes.
b) Learners can interact with, and are supported by, others in the programme's learning environments including peer learners, teachers, and where applicable supervisors, practitioners and mentors.
c) The programme includes arrangements to ensure that the parts of the programme that occur in the workplace are subject to the same rigours as any other part of the programme while having regard to the different nature of the workplace.

Programme	**Satisfactory? (yes, no, partially)**	**Comment**
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. A Student Experience Team is in place encompassing Careers, Student Services and International Student Services. This team has offices in two buildings (Castle House and Aungier Street) and aims to ensure that "DBS students have the best possible college-life experience and to promote a DBS community and culture that is focused on student wellbeing and success" (Programme Descriptor, Section 9.3, p. 93). DBS has established a Peer Mentor Programme, consisting of over 80 peer mentors, to enable learners to share their experiences of college life and act as positive role models for newer learners. Within the programme itself, guest speakers are often brought in to provide learners with industry insight and new perspectives on sectoral trends.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 9. There are sound teaching and learning strategies

a) The teaching strategies support achievement of the intended programme/module learning outcomes.
b) The programme provides authentic learning opportunities to enable learners to achieve the intended programme learning outcomes.
c) The programme enables enrolled learners to attain (if reasonably diligent) the minimum intended programme learning outcomes reliably and efficiently (in terms of overall learner effort and a reasonably balanced workload).
d) Learning is monitored/supervised.
e) Individualised guidance, support and timely formative feedback is regularly provided to enrolled learners as they progress within the programme.

Programme	**Satisfactory? (yes, no, partially)**	**Comment**
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. DBS has oriented the programme with a skills-based, practical focus. Accordingly, teaching and learning will heavily centre on problem-solving and critical reflection. Through lectures, workshops, tutorials and practical sessions, DBS hopes to encourage "learners to develop critical thinking, creative problem solving, and analytics and evaluative skills relating to real-world scenarios" (Programme Descriptor, Section 6.5, p. 59). As a means of encouraging peer review, the teaching and learning strategy incorporates a pairing approach for code review as well as peer review of academic articles. While formative assessment is utilised with the intent to provide constructive feedback, the Panel found that feedback was sometimes delivered late in a given module, meaning learners had no real opportunity to incorporate their learning from an assessment within the same module. This matter is explored further, with examples, under Criterion 10.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 10. There are sound assessment strategies

a) All assessment is undertaken consistently
b) The programme's assessment procedures interface effectively with the provider's QQI approved quality assurance procedures.
c) The programme includes specific procedures that are fair and consistent for the assessment of enrolled learners to ensure the minimum intended programme/module learning outcomes are acquired by all who successfully complete the programme.
d) The programme includes formative assessment to support learning.
e) There is a satisfactory written **programme assessment strategy** for the programme as a whole and there are satisfactory module assessment strategies for any of its constituent modules.
f) Sample assessment instruments, tasks, marking schemes and related evidence have been provided for each award-stage assessment and indicate that the assessment is likely to be valid and reliable.
g) There are sound procedures for the moderation of summative assessment results.
h) The provider only puts forward an enrolled learner for certification for a particular award for which a programme has been validated if they have been specifically assessed against the standard for that award.

Programme	Satisfactory? (yes, no, partially)	Comment
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. The assessment strategy for the programme is articulated in the Programme Descriptor and aligns with both the teaching and learning strategy and DBS' institutional assessment processes. A recurring item of feedback from learners concerned the timeliness and depth of assessment feedback, with some learners noting that feedback was not given until their last result, meaning there was no formative feedback they could draw upon to identify areas for enhancement in their own learning journey. One learner also appeared to indicate that errors in assignments were sometimes left unexplained, making it difficult to ascertain why a particular answer was incorrect (Programme Review Report, p. 77). Although DBS acknowledged timely feedback as important, the response given in the Programme Review Report did not sufficiently articulate its response to learner concerns, nor did it definitively explain whether DBS has actually implemented measures to improve the timeliness and depth of feedback (see Criterion 12 for further discussion on this matter). In respect of this, the Panel makes the following recommendation: **Recommendation 7** The Panel recommends that DBS review its approach to assessment feedback to ensure: a. Feedback is more consistently delivered within a reasonable timeframe.

		b. Feedback is provided at more frequent intervals during a module. c. The timing and depth of feedback is sufficient to help learners identify areas of strength and areas requiring further enhancement. -- In querying the absence of exams on the programme, DBS noted that the decision was made at School-level to remove exams for most Master's-level programmes. With regard to the MSc in Cybersecurity specifically, exams were considered less fit-for-purpose for getting learners work-ready, and given the programme's skills-based focus, it felt appropriate to design more practical assessments. While acknowledging DBS' stance on the matter, the Panel queried whether there may be instances in which exams could prove useful, as in module assessments where there is otherwise a risk of generative AI usage. DBS staff remarked that they want to avoid a knee-jerk reaction to generative AI and that there are guidelines in place at an institution-level which address its usage in assessment. In respect of this, the Panel makes the following recommendation: **Recommendation 8** The Panel recommends that DBS reflect on its decision to entirely remove exams from the programme.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 11. Learners enrolled on the programme are well informed, guided and cared for

a) There are arrangements to ensure that each enrolled learner is fully informed in a timely manner about the programme including the schedule of activities and assessments.
b) Information is provided about learner supports that are available to learners enrolled on the programme.
c) Specific information is provided to learners enrolled on the programme about any programme-specific appeals and complaints procedures.
d) If the programme is modular, it includes arrangements for the provision of effective guidance services for learners on the selection of appropriate learning pathways.
e) The programme takes into account and accommodates to the differences between enrolled learners, for example, in terms of their prior learning, maturity, and capabilities.
f) There are arrangements to ensure that learners enrolled on the programme are supervised and individualised support and due care is targeted at those who need it.
g) The programme provides supports for enrolled learners who have special education and training needs.
h) The programme makes reasonable accommodations for learners with disabilities.
i) If the programme aims to enrol international students it complies with the *Code of Practice for Provision of Programmes to International Students* and there are appropriate in-service supports in areas such as English language, learning skills, information technology skills and such like, to address the particular needs of international learners and enable such learners to successfully participate in the programme.
j) The programme's learners will be well cared for and safe while participating in the programme, (e.g. while at the provider's premises or those of any collaborators involved in provision, the programme's locations of provision including any workplace locations or practice-placement locations).

Programme	**Satisfactory? (yes, no, partially)**	**Comment**
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. DBS has a comprehensive range of services and resources in place to support learners and ensure the learner voice is represented within Governance. This includes a Student Council, a Class Rep system, a Peer Mentor Programme, Immigration Services, Accommodation Advice, Sports Clubs, Societies, a Learner Supports Services, and Academic Support Community, a Library Team, and a Student Engagement and Success Unit (SESU). The Academic Support Community, facilitated through the SESU, endeavours to improve the learner experience through the provision of peer to peer supports, academic supports, social supports, disabilities supports, and welfare supports.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Criterion 12. The programme is well managed

a) The programme includes intrinsic governance, quality assurance, learner assessment, and access, transfer and progression procedures that functionally interface with the provider's general or institutional procedures.
b) The programme interfaces effectively with the provider's QQI approved quality assurance procedures. Any proposed incremental changes to the provider's QA procedures required by the programme or programme-specific QA procedures have been developed having regard to QQI's statutory QA guidelines. If the QA procedures allow the provider to approve the centres within the provider that may provide the programme, the procedures and criteria for this should be fit-for-the-purpose of identifying which centres are suited to provide the programme and which are not.
c) There are explicit and suitable programme-specific criteria for selecting persons who meet the programme's staffing requirements and can be added to the programme's complement of staff.
d) There are explicit and suitable programme-specific criteria for selecting physical resources that meet the programmes physical resource requirements, and can be added to the programme's complement of supported physical resources.
e) Quality assurance is intrinsic to the programme's maintenance arrangements and addresses all aspects highlighted by the validation criteria.
f) The programme-specific quality assurance arrangements are consistent with QQI's statutory QA guidelines and use continually monitored completion rates and other sources of information that may provide insight into the quality and standards achieved.
g) The programme operation and management arrangements are coherently documented and suitable.
h) There are sound procedures for interface with QQI certification.

Programme	Satisfactory? (yes, no, partially)	Comment
MSc in Cybersecurity	Yes	The Panel is satisfied that QQI's requirements under this criterion have been addressed. DBS has well-established quality assurance procedures underpinning the provision of the programme and the Panel is satisfied that the programme interfaces functionally with these procedures. DBS has also developed guidelines for learners on the use of generative AI in assessment. The Panel recognises the value of these guidelines and is of the view that guidelines for faculty on how to teach and assess in the age of generative AI would be valuable and complementary to the learner-facing guidelines. In respect of this, the Panel makes the following recommendation: **Recommendation 9** The Panel recommends that DBS consider developing and instituting guidelines for faculty on how to teach and assess in the age of generative AI (which may complement the existing learner-facing guidelines on gen AI use). -- Given the significant year on year growth in applications (from 164 in 2020/21 to 1,237 in 2023/24), enrolment numbers have increased more than tenfold over the same

		period. DBS has articulated its intention to further grow the programme, with the Programme Descriptor stating that DBS can accommodate a maximum of 120 learners per intake across 3 proposed intakes on the full-time version of the programme and 2 proposed intakes on the part-time version of the programme, up to a total 600 learners per year. The Panel is cognisant that these numbers do not strictly represent a target; nonetheless, it is crucial that DBS closely observes its capacity and resource availability in view of its intention to grow the programme. In respect of this, the Panel makes the following recommendation: **Recommendation 10** Considering DBS' strategic intent to increase enrolment numbers over the next validation period, the Panel recommends that DBS closely monitor its capacity and resource availability (physical and human) to ensure these remain viable. -- As discussed in the Panel's report on DBS' programme review process, there was an observed gender imbalance over the last validation period. Though improving year on year, the programme commenced in 2020/21 with a 100% male cohort which, over the next three years, would become a 77.60% male to 22.40% female cohort in the 2023/24 academic year. DBS recognises this as an area requiring further attention, but also acknowledges the imbalance as indicative of a broader trend in STEM fields. In respect of this, the Panel makes the following recommendation: **Recommendation 11** The Panel recommends that DBS give further consideration to how it can improve the gender balance on the programme, in relation to staff and students. -- During the Panel's initial evaluation of the Programme Review Report, there was a noted absence of tangible data concerning complaints and appeals over the last validation period and whether complaints and appeals, if any, had been resolved in line with defined procedures. Instead, the Programme Review Report articulated DBS' definition of complaints and appeals and the learner's right to pursue these as appropriate.

		This omission was raised with DBS staff during the site visit who acknowledged the omission and later provided the Panel with a spreadsheet detailing the figures for complaints and appeals since the 2020/21 academic year. As a matter of good practice, the Panel advises that this data be included in future programme review reports for transparency. In respect of this, the Panel makes the following recommendation: **Recommendation 12** The Panel recommends that DBS include details about the number of complaints and appeals received over the last validation period within the Programme Review Report, and indicate whether these were resolved in accordance with defined procedures, even if this number is zero. -- The Panel observed a number of instances in the Programme Review Report in which the language used (particularly advisory and speculative modal verbs) creates ambiguity for the reader in understanding whether certain actions have been applied, and if they have been applied, to what extent. One such example is found in Section 4.1.3 (p. 88) relating to assessment feedback timelines and states, "The programme **should** strive to provide timely and constructive feedback to students..." and "This **might** involve setting clear expectations for feedback turnaround time...". Another example in the same section notes that there is a desire for more practical experience, to which DBS' response is: "This **could** involve incorporating dedicated modules or workshops focused on specific tools..." In respect of this, the Panel makes the following recommendation: **Recommendation 13** The Panel recommends that DBS review its use of language in the Programme Review Report to ensure it is clear whether an action has been implemented and to what extent.
PG Dip in Science in Cybersecurity	Yes	As per principal programme.

Part 3. Overall recommendation to QQI

3.1 Principal programme: Master of Science in Cybersecurity

Select one	
X	Satisfactory (meaning that it recommends that QQI can be satisfied in the context of unit 2.3) of Core policies and criteria for the validation by QQI of programmes of education and training;
	Satisfactory subject to proposed special conditions (specified with timescale for compliance for each condition; these may include proposed pre-validation conditions i.e. proposed (**minor**) things to be done to a programme that almost fully meets the validation criteria before QQI makes a determination);
	Not satisfactory.

Reasons for the overall recommendation

The programme fully meets the validation criteria.

Commendations

1. The Panel commends:
    a. DBS' constructive engagement with the Panel during the site visit.
    b. The relevance and currency of the programme's content.

Special Conditions of Validation (directive and with timescale for compliance)

No special conditions of validation identified.

Recommendations

1. The Panel recommends that DBS consider offering elective modules to meet the needs of learners with different career ambitions.

2. The Panel recommends that DBS reconsider its decision to include two modules on research methods given the mostly practical, skills-based focus of the programme.

3. In relation to the Advanced Programming Techniques module, the Panel recommends:
    a. that DBS reconsider the use of the word 'Advanced' in the title.
    b. that DBS more visibly cover secure software in the module content.
    c. that DBS review the current group assessment worth 70% of the overall grade to ensure that this is an authentic assessment.

4. The Panel recommends that DBS consider the inclusion of additional modules around cybersecurity.

5. The Panel recommends that DBS more clearly articulates the coverage of operational technology standards, policy and risk analysis within the indicative module content.

6. The Panel recommends that DBS incorporates the most recent EU legislation and regulations on cybersecurity within the programme.

7. The Panel recommends that DBS review its approach to assessment feedback to ensure:

    a. Feedback is more consistently delivered within a reasonable timeframe.

b. Feedback is provided at more frequent intervals during a module.
c. The timing and depth of feedback is sufficient to help learners identify areas of strength and areas requiring further enhancement.

8. The Panel recommends that DBS reflect on its decision to entirely remove exams from the programme.

9. The Panel recommends that DBS consider developing and instituting guidelines for faculty on how to teach and assess in the age of generative AI (which may complement the existing learner-facing guidelines on gen AI use).

10. Considering DBS' strategic intent to increase enrolment numbers over the next validation period, the Panel recommends that DBS closely monitor its capacity and resource availability (physical and human) to ensure these remain viable.

11. The Panel recommends that DBS give further consideration to how it can improve the gender balance on the programme, in relation to staff and students.

12. The Panel recommends that DBS include details about the number of complaints and appeals received over the last validation period within the Programme Review Report, and indicate whether these were resolved in accordance with defined procedures, even if this number is zero.

13. The Panel recommends that DBS review its use of language in the Programme Review Report to ensure it is clear whether an action has been implemented and to what extent.

Embedded programme: Postgraduate Diploma in Science in Cybersecurity

Select one	
X	Satisfactory (meaning that it recommends that QQI can be satisfied in the context of unit 2.3) of Core policies and criteria for the validation by QQI of programmes of education and training;
	Satisfactory subject to proposed special conditions (specified with timescale for compliance for each condition; these may include proposed pre-validation conditions i.e. proposed (**minor**) things to be done to a programme that almost fully meets the validation criteria before QQI makes a determination);
	Not satisfactory.

Reasons for the overall recommendation

The programme fully meets the validation criteria.

Commendations

1. The Panel commends:
    a. DBS' constructive engagement with the Panel during the site visit.
    b. The relevance and currency of the programme's content.

Special Conditions of Validation (directive and with timescale for compliance)

No special conditions of validation identified.

Recommendations

1. The Panel recommends that DBS consider offering elective modules to meet the needs of learners with different career ambitions.

2. The Panel recommends that DBS reconsider its decision to include two modules on research methods given the mostly practical, skills-based focus of the programme.

3. In relation to the Advanced Programming Techniques module, the Panel recommends:
    a. that DBS reconsider the use of the word 'Advanced' in the title.
    b. that DBS more visibly cover secure software in the module content.
    c. that DBS review the current group assessment worth 70% of the overall grade to ensure that this is an authentic assessment.

4. The Panel recommends that DBS consider the inclusion of additional modules around cybersecurity.

5. The Panel recommends that DBS more clearly articulates the coverage of operational technology standards, policy and risk analysis within the indicative module content.

6. The Panel recommends that DBS incorporates the most recent EU legislation and regulations on cybersecurity within the programme.

7. The Panel recommends that DBS review its approach to assessment feedback to ensure:

    a. Feedback is more consistently delivered within a reasonable timeframe.

b. Feedback is provided at more frequent intervals during a module.
c. The timing and depth of feedback is sufficient to help learners identify areas of strength and areas requiring further enhancement.

8. The Panel recommends that DBS reflect on its decision to entirely remove exams from the programme.

9. The Panel recommends that DBS consider developing and instituting guidelines for faculty on how to teach and assess in the age of generative AI (which may complement the existing learner-facing guidelines on gen AI use).

10. Considering DBS' strategic intent to increase enrolment numbers over the next validation period, the Panel recommends that DBS closely monitor its capacity and resource availability (physical and human) to ensure these remain viable.

11. The Panel recommends that DBS give further consideration to how it can improve the gender balance on the programme, in relation to staff and students.

12. The Panel recommends that DBS include details about the number of complaints and appeals received over the last validation period within the Programme Review Report, and indicate whether these were resolved in accordance with defined procedures, even if this number is zero.

13. The Panel recommends that DBS review its use of language in the Programme Review Report to ensure it is clear whether an action has been implemented and to what extent.

Summary of recommended special conditions of validation

No special conditions of validation identified.

Summary of recommendations to the provider

1. The Panel recommends that DBS consider offering elective modules to meet the needs of learners with different career ambitions.

2. The Panel recommends that DBS reconsider its decision to include two modules on research methods given the mostly practical, skills-based focus of the programme.

3. In relation to the Advanced Programming Techniques module, the Panel recommends:
    a. that DBS reconsider the use of the word 'Advanced' in the title.
    b. that DBS more visibly cover secure software in the module content.
    c. that DBS review the current group assessment worth 70% of the overall grade to ensure that this is an authentic assessment.

4. The Panel recommends that DBS consider the inclusion of additional modules around cybersecurity.

5. The Panel recommends that DBS more clearly articulates the coverage of operational technology standards, policy and risk analysis within the indicative module content.

6. The Panel recommends that DBS incorporates the most recent EU legislation and regulations on cybersecurity within the programme.

7. The Panel recommends that DBS review its approach to assessment feedback to ensure:

    a. Feedback is more consistently delivered within a reasonable timeframe.
    b. Feedback is provided at more frequent intervals during a module.
    c. The timing and depth of feedback is sufficient to help learners identify areas of strength and areas requiring further enhancement.
8. The Panel recommends that DBS reflect on its decision to entirely remove exams from the programme.

9. The Panel recommends that DBS consider developing and instituting guidelines for faculty on how to teach and assess in the age of generative AI (which may complement the existing learner-facing guidelines on gen AI use).

10. Considering DBS' strategic intent to increase enrolment numbers over the next validation period, the Panel recommends that DBS closely monitor its capacity and resource availability (physical and human) to ensure these remain viable.

11. The Panel recommends that DBS give further consideration to how it can improve the gender balance on the programme, in relation to staff and students.

12. The Panel recommends that DBS include details about the number of complaints and appeals received over the last validation period within the Programme Review Report, and

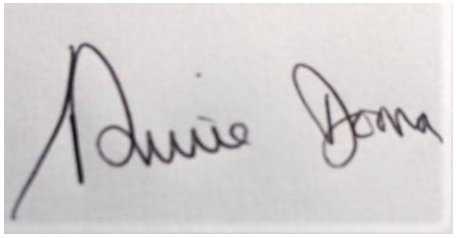
whether these were resolved in accordance with defined procedures, even if this number is zero.

13. The Panel recommends that DBS review its use of language in the Programme Review Report to ensure it is clear whether an action has been implemented and to what extent.

Declarations of Evaluators' Interests

This report has been agreed by the evaluation panel and is signed on their behalf by the chairperson.

Panel chairperson: Dr Annie Doona Date: 13th February 2025

Signed: 

3.2 Disclaimer

The Report of the External Review Panel contains no assurances, warranties or representations express or implied, regarding the aforesaid issues, or any other issues outside the Terms of Reference.

While QQI has endeavoured to ensure that the information contained in the Report is correct, complete and up-to-date, any reliance placed on such information is strictly at the reader's own risk, and in no event will QQI be liable for any loss or damage (including without limitation, indirect or consequential loss or damage) arising from, or in connection with, the use of the information contained in the Report of the External Evaluation Panel.

Part 4. Proposed programme schedules *(post panel feedback and consequent amendments, if any)*

4a Proposed Programme Schedule(s) - FULL TIME						
Name of Provider:	Dublin Business School					
Programme Title *(Principal)*	MSc in Cybersecurity		**QQI Award Title**	Master of Science	**ECTS**	90
Stage (1,2,3, Award etc)	Award	**Exit Award Title** *(if relevant)*	Postgraduate Diploma in Science in Cybersecurity		**Stage ECTS**	90

Programme Delivery Mode - ✔ *one as appropriate.*	**On-site Face-to-Face**	**Blended**	**Online**	**Apprenticeship**
		✔		

Teaching and Learning Modalities – ✔ *one or more as appropriate.*	**On-site Face-to-Face**	**Synchronous Hybrid**	**Synchronous Online**	**Asynchronous**	**Independent**	**Work Based**
	✔		✔	✔	✔	

Assessment Techniques Utilised in Stage – ✔ *one or more as appropriate.*	**Continuous Assessment**	**Invigilated Exam – in person**	**Proctored Exam - online**	**Project**	**Practical Skills Demonstration**	**Work Based**
	✔			✔		

Modules in this stage (add rows as required)

	Total Student Effort Module (hours)	**Assessment – Allocation of Marks** *(from the module assessment strategy)*

Module Title	**Semester**	**Mandatory (M) or Elective (E)**	**Credits (ECTS)**	**Total Hours**	**On-site Face-to-Face**	**Synchronous**	**Asynchronous**	**Independent**	**Work Based**	**Continuous Assessment %**	**Invigilated Exam – in person %**	**Proctored Exam – online %**	**Project**	**Practical Skills Demonstration %**	**Work Based %**
Advanced Programming Techniques	1	M	5	125	24			101		100%					
Advanced Databases	1	M	5	125	24			101		100%					
Networks and Systems Administration	1	M	5	125	24			101		100%					

Cryptography & Digital Forensics	1	M	10	250	36	12		202		100%					
Cybersecurity Research: Threats, Technologies, and Governance	1	M	5	125	24			101		100%					
Communications and Networking Security	2	M	10	250	36	12		202		100%					
Cybersecurity for Software Development	2	M	5	125	24			101		100%					
Penetration Testing and Business Continuity Management	2	M	5	125	24			101		100%					
Organisational and Societal Cybersecurity	2	M	10	250	36	12		202		100%					
Applied Research Methods	2	M	5	125	24			101		100%					
Applied Research Project	3	E	25	625	6			619					100%		
Dissertation	3	E	25	625	6			619					100%		

4b Proposed Programme Schedule(s) - PART TIME

Name of Provider:	Dublin Business School					
Programme Title *(Principal)*	MSc in Cybersecurity		**QQI Award Title**	Master of Science	**ECTS**	90
Stage (1,2,3, Award etc)	Award	**Exit Award Title** *(if relevant)*	Postgraduate Diploma in Science in Cybersecurity		**Stage ECTS**	90

Programme Delivery Mode - ✔ *one as appropriate.*	**On-site Face-to-Face**	**Blended**	**Online**	**Apprenticeship**
		✔		

Teaching and Learning Modalities – ✔ *one or more as appropriate.*	**On-site Face-to-Face**	**Synchronous Hybrid**	**Synchronous Online**	**Asynchronous**	**Independent**	**Work Based**
	✔		✔	✔	✔	
Assessment Techniques Utilised in Stage – ✔ *one or more as appropriate.*	**Continuous Assessment**	**Invigilated Exam – in person**	**Proctored Exam - online**	**Project**	**Practical Skills Demonstration**	**Work Based**
	✔			✔		

Modules in this stage (add rows as required)

					Total Student Effort Module (hours)					**Assessment – Allocation of Marks** *(from the module assessment strategy)*					
Module Title	**Semester**	**Mandatory (M) or Elective (E)**	**Credits (ECTS)**	**Total Hours**	**On-site Face-to-Face**	**Synchronous**	**Asynchronous**	**Independent**	**Work Based**	**Continuous Assessment %**	**Invigilated Exam – in person %**	**Proctored Exam – online %**	**Project**	**Practical Skills Demonstration %**	**Work Based %**
Advanced Programming Techniques	1	M	5	125	3	15		107		100%					
Advanced Databases	1	M	5	125	3	15		107		100%					
Networks and Systems Administration	1	M	5	125	3	15		107		100%					
Cryptography & Digital Forensics	2	M	10	250	3	33		214		100%					
Cybersecurity Research: Threats, Technologies, and Governance	2	M	5	125	3	15		107		100%					
Communications and Networking Security	3	M	10	250	3	33		214		100%					
Cybersecurity for Software Development	3	M	5	125	3	15		107		100%					

Penetration Testing and Business Continuity Management	4	M	5	125	3	15		107		100%					
Organisational and Societal Cybersecurity	4	M	10	250	3	33		214		100%					
Applied Research Methods	4	M	5	125	3	15		107		100%					
Applied Research Project	5	E	25	625	6			619					100%		
Dissertation	5	E	25	625	6			619					100%		

Postgraduate Diploma in Science in Cybersecurity Full- and Part-Time

4c Proposed Programme Schedule(s) - FULL TIME						
Name of Provider:	Dublin Business School					
Programme Title *(Principal)*	Postgraduate Diploma in Science in Cybersecurity	**QQI Award Title**	Postgraduate Diploma in Science		**ECTS**	60
Stage (1,2,3, Award etc)	Award	**Exit Award Title** *(if relevant)*	NA		**Stage ECTS**	60

Programme Delivery Mode - ✔ *one as appropriate.*	**On-site Face-to-Face**	**Blended**	**Online**	**Apprenticeship**
		✔		

Teaching and Learning Modalities – ✔ *one or more as appropriate.*	**On-site Face-to-Face**	**Synchronous Hybrid**	**Synchronous Online**	**Asynchronous**	**Independent**	**Work Based**
	✔		✔	✔	✔	

Assessment Techniques Utilised in Stage – ✔ *one or more as appropriate.*	**Continuous Assessment**	**Invigilated Exam – in person**	**Proctored Exam - online**	**Project**	**Practical Skills Demonstration**	**Work Based**
	✔			✔		

Modules in this stage (add rows as required)		
	Total Student Effort Module (hours)	**Assessment – Allocation of Marks** *(from the module assessment strategy)*

Module Title	Semester	Mandatory (M) or Elective (E)	Credits (ECTS)	Total Hours	On-site Face-to-Face	Synchronous	Asynchronous	Independent	Work Based	Continuous Assessment %	Invigilated Exam – in person %	Proctored Exam – online %	Project	Practical Skills Demonstration %	Work Based %
Advanced Programming Techniques	1	M	5	125	24			101		100%					
Advanced Databases	1	M	5	125	24			101		100%					
Networks and Systems Administration	1	M	5	125	24			101		100%					
Cryptography & Digital Forensics	1	M	10	250	36	12		202		100%					
Cybersecurity Research: Threats, Technologies, and Governance	1	M	5	125	24			101		100%					
Communications and Networking Security	2	M	10	250	36	12		202		100%					
Cybersecurity for Software Development	2	M	5	125	24			101		100%					
Penetration Testing and Business Continuity Management	2	M	5	125	24			101		100%					
Organisational and Societal Cybersecurity	2	M	10	250	36	12		202		100%					

4d	**Proposed Programme Schedule(s) - PART TIME** Dublin Business School													
Programme Title *(Principal)*	Postgraduate Diploma in Science in Cybersecurity			**QQI Award Title**	Postgraduate Diploma in Science							**ECTS**	60	
Stage (1,2,3, Award etc)	Award		**Exit Award Title** *(if relevant)*	NA								**Stage ECTS**	60	
Programme Delivery Mode - ✔ *one as appropriate.*	**On-site Face-to-Face**		**Blended**		**Online**		**Apprenticeship**							
			✔											
Teaching and Learning Modalities – ✔ *one or more as appropriate.*	**On-site Face-to-Face**		**Synchronous Hybrid**		**Synchronous Online**		**Asynchronous**		**Independent**		**Work Based**			
	✔				✔		✔		✔					
Assessment Techniques Utilised in Stage – ✔ *one or more as appropriate.*	**Continuous Assessment**		**Invigilated Exam – in person**		**Proctored Exam - online**		**Project**		**Practical Skills Demonstration**		**Work Based**			
	✔						✔							
Modules in this stage (add rows as required)														
				Total Student Effort Module (hours)						**Assessment – Allocation of Marks** *(from the module assessment strategy)*				
Module Title	**Semester**	**Mandatory (M) or Elective (E)**	**Credits (ECTS)**	**Total Hours**	**On-site Face-to-Face**	**Synchronous**	**Asynchronous**	**Independent**	**Work Based**	**Continuous Assessment %**	**Invigilated Exam – in person %**	**Proctored Exam – online %**	**Project**	**Practical Skills Demonstration %**	**Work Based %**
Advanced Programming Techniques	1	M	5	125	3	15		107		100%					
Advanced Databases	1	M	5	125	3	15		107		100%					
Networks and Systems Administration	1	M	5	125	3	15		107		100%					
Cryptography & Digital Forensics	2	M	10	250	3	33		214		100%					
Cybersecurity Research:	2	M	5	125	3	15		107		100%					

Threats, Technologies, and Governance															
Communications and Networking Security	3	M	10	250	3	33		214		100%					
Cybersecurity for Software Development	3	M	5	125	3	15		107		100%					
Penetration Testing and Business Continuity Management	4	M	5	125	3	15		107		100%					
Organisational and Societal Cybersecurity	4	M	10	250	3	33		214		100%					