Dearbhú Cáilíochta agus Cáilíochtaí Éireann
Quality and Qualifications Ireland

CERTIFICATE OF VALIDATION

New validation

Validation Process: **Revalidation**

Provider Name	Dublin Business School
Date of Validation	10-Jun-25

	Code	Title	Award	Exit Only
Principal Programme	PG26319	Master of Science in Cybersecurity	Master of Science (Masters Degree at NFQ Level 9) 9M22928 90 credits	N/A
Embedded Programme	PG26320	Postgraduate Diploma in Science in Cybersecurity	Postgraduate Diploma in Science (Postgraduate Diploma at NFQ Level 9) 9M22926 60 credits	Yes

	First Intake	Last Intake
Enrolment Interval	Sep-25	Aug-30

Principal Programme

	Full Time	Part Time
Intakes per Annum:	3	2
Minimum Learners per Intake:	10	10
Maximum Learners per Intake:	120	120
Duration (months)	12	24

Delivery Mode: full-time / part-time	Full Time, Part Time

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.

Brief Synopsis of the Programmes

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 Masters programme.

Minimum Intended Programme Learning Outcomes

On completion of this programme the learner will be able to:

1. Exhibit an extensive knowledge of the theoretical and conceptual knowledge essentials in the discipline of cybersecurity.
2. Critically analyse a range of methods, tools and technologies identifying strengths and weaknesses within current security standards.
3. Evidence critical awareness of emerging tools, trends and technologies in the constantly emerging area of cybersecurity, including the areas of law and ethics.
4. Evidence advanced skills that are required in the design, development, evaluation and security of cybersecurity in a modern computing environment.
5. Interpret complex security models and methodologies into unfamiliar situations in order to devise effective technical and nontechnical solutions appropriate for strategic security recommendations.
6. Exhibit a critical awareness of technological, political, social, regulatory and economic developments affecting the cybersecurity environment.
7. Develop effective communication, time-management, teamwork and leadership abilities suitable for a professional environment.
8. Support continuing professional development to ensure that key considerations and implications of 'own work' and 'work of others' are in the best interests of all stakeholders through maintaining integrity and independence in professional judgement.
9. Evolve problem-solving skills to address clients' problems and provide solutions by using existing research and applying suitable research methods.
10. Demonstrate proficiency in research skills to plan, design, develop and manage a research project that demonstrates competencies in cybersecurity and comply with the ethical implications in the relevant domain.

Teaching and Learning Modes	1. Lectures / Classes 2. Practical Sessions 3. Tutorials

Approved Countries	Ireland

Physical Resource Requirements

Appropriately equipped computer work area.

Lecture rooms of sufficient size for work in breakout groups/with appropriate multimedia resources.

Appropriate software resources to be used in the teaching and learning of all modules.

Learners are also required to have ongoing access to a computer, related software, and a reliable internet connection. This means that for learners their laptop or desktop computer will require a minimum of a supported version of a Windows operating system and 4GM RAM.

Staff Profiles	Qualifications and Experience	WTE
Lecturer	Lecturing staff will have a minimum of a Masters and/or PhD in the following areas: Computing science / Computing Quantitative methods Cybersecurity Networking Information Systems Computer Technology Research methods Mathematics and statistics In modules where industry experience is desirable, those who are exceptionally qualified by virtue of senior significant experience may also be considered.	10
Academic Director	The Academic Director will be responsible for the overall management and development of the programme, the coordination of the organisation and delivery of the programme, and the management and support of learners on the programme through Assistant Academic Directors and Programme Level Managers. The Academic Director is responsible for the suite of programmes in their discipline area and ensures programme offerings are current, employment-focused and academically robust and coherent in construct. The Academic Director provides academic leadership to Faculty and to Programme Teams in the development and delivery of high-quality, progressive, learner-centred education. The Academic Director role is focused around 3 distinct areas: Governance of discipline area programmes. Programme development, review, and retention for discipline areas. Programme innovation, employer engagement and foster business opportunity in the discipline area.	1
Assistant Academic Director	The Assistant Academic Director works alongside the Academic Director across many of their duties, including the management and development of the programme, the coordination of the organisation and delivery of the programme, and the management and support of learners on the programme. The Assistant Academic Director also works in a student-facing capacity, through teaching and supporting students more generally throughout their time as DBS. The Assistant Academic Director role is focused around 3 distinct areas: Effective programme management and teaching, learning and assessment initiatives in DBS programmes. Implementation of programme development, review, and retention initiatives in the discipline area. Supporting the discipline Academic Director in discipline development, enhancement and innovation including opportunities for business development, employer-facing initiatives and improved graduate outcomes.	1
Programme Level Manager	The Programme Level Manager (PLM) provides professional leadership and management for an allocated subject area in order to facilitate teaching and learning and to secure effective use of resources. This includes undertaking teaching duties as appropriate to the requirements of a programme and consistent with the area(s) of expertise, keeping up-to-date with teaching and learning developments and being alert to best practice, providing guidance to colleagues on content, methodology and resources regarding the subject area and answering subject specific queries and requests for accommodations from learners.	1

Approved Centres	Centre	Minimum Enrolment per Annum	Maximum Enrolment per Annum
	38628L Dublin Business School	10	600

Additional Locations	Location Name	Minimum Enrolment per Annum	Maximum Enrolment per Annum
	N/A		

Learner Teacher Ratios	Learning Activity	Ratio
	Lecture classroom-based sessions	1:60
	Practical lab sessions	1:30
	Online class sessions	1:60

Programme being replaced by this Programme	Prog Code	Programme Title	Validated
	PG24326	Master of Science in Cybersecurity	25-Apr-24

Embedded Programme

Validation Process: **Revalidation**

Code	Title	Award	Exit Only
PG26320	Postgraduate Diploma in Science in Cybersecurity	Postgraduate Diploma in Science (Postgraduate Diploma at NFQ Level 9) 9M22926 60 credits	Yes

	Full Time	Part Time
Duration (months)	9	18

Delivery Mode: full-time / part-time	Full Time, Part Time

Target Learner Groups

The Postgraduate Diploma is offered as an exit award for learners who cannot complete the full Master's programme.

Brief Synopsis of the Programmes

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.

Minimum Intended Programme Learning Outcomes

On completion of this programme the learner will be able to:

1. Exhibit an extensive knowledge of the theoretical and conceptual knowledge essentials in the discipline of cybersecurity.
2. Critically analyse a range of methods, tools and technologies identifying strengths and weaknesses within current security standards.
3. Evidence critical awareness of emerging tools, trends and technologies in the constantly emerging area of cybersecurity, including the areas of law and ethics.
4. Evidence advanced skills that are required in the design, development, evaluation and security of cybersecurity in a modern computing environment.
5. Interpret complex security models and methodologies into unfamiliar situations in order to devise effective technical and nontechnical solutions appropriate for strategic security recommendations.
6. Exhibit a critical awareness of technological, political, social, regulatory and economic developments affecting the cybersecurity environment.
7. Develop effective communication, time-management, teamwork and leadership abilities suitable for a professional environment.
8. Support continuing professional development to ensure that key considerations and implications of 'own work' and 'work of others' are in the best interests of all stakeholders through maintaining integrity and independence in professional judgement.
9. Evolve problem-solving skills to address clients' problems and provide solutions by using existing research and applying suitable research methods.

Teaching and Learning Modes	1. Lectures / Classes 2. Practical Sessions 3. Tutorials

Approved Countries	Ireland

Physical Resource Requirements

Appropriately equipped computer work area.

Lecture rooms of sufficient size for work in breakout groups/with appropriate multimedia resources.

Appropriate software resources to be used in the teaching and learning of all modules.

Learners are also required to have ongoing access to a computer, related software, and a reliable internet connection. This means that for learners their laptop or desktop computer will require a minimum of a supported version of a Windows operating system and 4GM RAM.

Staff Profiles	Qualifications and Experience	WTE
Lecturer	Lecturing staff will have a minimum of a Masters and/or PhD in the following areas: Computing science / Computing Quantitative methods Cybersecurity Networking Information Systems Computer Technology Research methods Mathematics and statistics In modules where industry experience is desirable, those who are exceptionally qualified by virtue of senior significant experience may also be considered.	10
Academic Director	The Academic Director will be responsible for the overall management and development of the programme, the coordination of the organisation and delivery of the programme, and the management and support of learners on the programme through Assistant Academic Directors and Programme Level Managers. The Academic Director is responsible for the suite of programmes in their discipline area and ensures programme offerings are current, employment-focused and academically robust and coherent in construct. The Academic Director provides academic leadership to Faculty and to Programme Teams in the development and delivery of high-quality, progressive, learner-centred education. The Academic Director role is focused around 3 distinct areas: Governance of discipline area programmes. Programme development, review, and retention for discipline areas. Programme innovation, employer engagement and foster business opportunity in the discipline area.	1
Assistant Academic Director	The Assistant Academic Director works alongside the Academic Director across many of their duties, including the management and development of the programme, the coordination of the organisation and delivery of the programme, and the management and support of learners on the programme. The Assistant Academic Director also works in a student-facing capacity, through teaching and supporting students more generally throughout their time as DBS. The Assistant Academic Director role is focused around 3 distinct areas: Effective programme management and teaching, learning and assessment initiatives in DBS programmes. Implementation of programme development, review, and retention initiatives in the discipline area. Supporting the discipline Academic Director in discipline development, enhancement and innovation including opportunities for business development, employer-facing initiatives and improved graduate outcomes.	1
Programme Level Manager	The Programme Level Manager (PLM) provides professional leadership and management for an allocated subject area in order to facilitate teaching and learning and to secure effective use of resources. This includes undertaking teaching duties as appropriate to the requirements of a programme and consistent with the area(s) of expertise, keeping up-to-date with teaching and learning developments and being alert to best practice, providing guidance to colleagues on content, methodology and resources regarding the subject area and answering subject specific queries and requests for accommodations from learners.	1

Approved Centres	Centre	Minimum Enrolment per Annum	Maximum Enrolment per Annum
	38628L Dublin Business School	0	0

Additional Locations	Location Name	Minimum Enrolment per Annum	Maximum Enrolment per Annum
	N/A		

Learner Teacher Ratios	Learning Activity	Ratio
	Lecture classroom-based sessions	1:60
	Practical lab sessions	1:30
	Online class sessions	1:60

Programme being replaced by this Programme	Prog Code	Programme Title	Validated
	PG24327	Postgraduate Diploma in Science in Cybersecurity	15-Oct-20

Conditions of Validation of the Programmes Covered by this Certificate of Validation

Part 1: Statutory Conditions of Validation

The statutory (section 45(3) of the 2012 Act) conditions of validation are that the provider of the programme shall:

1. Co-operate with and assist QQI in the performance of QQI's functions in so far as those functions relate to the functions of the provider,
2. Establish procedures which are fair and consistent for the assessment of enrolled learners to ensure the standards of knowledge, skill or competence determined by QQI under section 49 (1) are acquired, and where appropriate, demonstrated, by enrolled learners,
3. Continue to comply with section 65 of the 2012 Act in respect of arrangements for the protection of enrolled learners, if applicable, and
4. Provide to QQI such information as QQI may from time to time require for the purposes of the performance of its functions, including information in respect of completion rates.

Part 2 Conditions of Validation Established by QQI Under section 45(4)(b) of the 2012 Act)

Part 2.1 Condition of Validation Concerning a Change in the QQI Award or Award Standard

1. Where QQI changes an award title, an award specification or an award standard that a programme depends upon, the provider shall not enrol any further learners on the affected programmes unless informed otherwise in writing by QQI (e.g. by the issue of a revised certificate of validation). The programme is considered validated for learners already enrolled on the affected programme.

Part 2.2 Condition of Validation Concerning the Duration of Enrolment

1.The duration of enrolment is the interval during which learners may be enrolled on the validated programme.

Validation is determined by QQI for a specified number of years of enrolment appropriate to the particular programme as indicated on the certificate on validation subject to unit 9.2.1. It is a condition of validation that the programme does not enrol any new learners outside this interval. A typical duration would be five years.

If a provider wishes to continue to enrol learners to the programme beyond this interval the provider must arrange in good time for it to be validated again by QQI, or exceptionally the provider may apply for extension of the duration of enrolment (unit (14)). In this context the provider may apply for validation of the programme from first principles or, alternatively, the provider may avail of the process for revalidation (unit (13)) by QQI.

Part 2.3 General Condition of Validation

The provider of the programme shall:

1. Ensure that the programme as implemented does not differ in a material way from the programme as validated; differing in a material way is defined as differing in any aspect of the programme or its implementation that was material to QQI's validation criteria.
2. Ensure that the programme is provided with the appropriate staff and physical resources as validated.
3. Implement in respect of the programme its written quality assurance procedures (as approved by QQI).
4. Make no significant change to the programme without the prior approval of QQI. (See unit (8)).
5. Unless otherwise agreed by QQI in writting, start implementing the programme as validated and enrol learners within 18 months of validation.
6. Continue in respect of the validated programme to comply with section 56 of the 2012 Act in respect of procedures for access, transfer and progression.
7. Implement the programme and procedures for assessment of learners in accordance with the Approved Programme Schedule and notify QQI in writing of any amendments to this arising from changes to the programme; see unit (9).
8. When advertising and promoting the programme and awards, use the programme title as validated, and the correct QQI award title(s), award type(s) and award class(es) indicating the level of the award(s) on the National Framework of Qualifications.

9. Adhere to QQI regulations and procedures for certfication.
10. Notify QQI in writing without delay of: a. Any material change to the programme; a. Anything that impacts on the integrity or reputation of the programme or the corresponding QQI awards; b. Anything that infringes the conditions of validation; or c. Anything that would be likely to cause QQI to consider reviewing the validation.
11. Notify QQI in writing to determine the implications for the provider's validated programmes, where the provider is likely to, or planning to, merge (amalgamate) with another entity or to acquire, or be acquired by, another entity (see unit (12.5)) .
12. Report to QQI, when required or requested, on its implementation of the programme and compliance with the conditions of validation.

Part 2.4 General Condition of Validation Arising from Specialised Validation Policy and Criteria

Part 2.5 Special Conditions of Validation

Dearbhú Cáilíochta agus Cáilíochtaí Éireann
Quality and Qualifications Ireland

Programme and stage schedules

PG26319 Master of Science in Cybersecurity

Name of Provider	Dublin Business School							
Programme Title	PG26319 Master of Science in Cybersecurity							
Award Title	Master of Science					**Exit Award Only**	N/A	
Teaching and learning modalities	Lectures / Classes; Practical Sessions; Tutorials							
Delivery Modes	**Award Class**	**Award NFQ Level**	**Award EQF Level**	**Stage**	**Stage NFQ Level**	**Stage Credits**	**First Intake**	**ISCED Code**
Both	Major	9	7	Award Stage	9	90	Sep 2025	06.1.1

Module				**Total Student Effort Module (Hours)**					**Allocation of Marks**				
Title	**Semester**	**Status**	**Credit**	**Total Hours**	**Class Contact Hours**	**Direct e-learning**	**Hours of independent learning**	**Work-based learning efforts**	**C.A. %**	**Project %**	**Skills demonstration %**	**Exam %**	**Workbased %**
Advanced Programming Techniques	1	M	5	125	24	0	101	0	100	0	0	0	0
Advanced Databases	1	M	5	125	24	0	101	0	100	0	0	0	0
Networks and Systems Administration	1	M	5	125	24	0	101	0	100	0	0	0	0
Cryptography & Digital Forensics	1	M	10	250	48	0	202	0	100	0	0	0	0
Cybersecurity Research: Threats, Technologies, and	1	M	5	125	24	0	101	0	100	0	0	0	0
Communications and Networking Security	2	M	10	250	48	0	202	0	100	0	0	0	0
Cybersecurity for Software Development	2	M	5	125	24	0	101	0	100	0	0	0	0
Penetration Testing and Business Continuity Manage	2	M	5	125	24	0	101	0	100	0	0	0	0
Organisational and Societal Cybersecurity	2	M	10	250	48	0	202	0	100	0	0	0	0
Applied Research Methods	2	M	5	125	24	0	101	0	100	0	0	0	0
Applied Research Project	3	E	25	625	6	0	619	0	0	100	0	0	0
Dissertation	3	E	25	625	6	0	619	0	0	100	0	0	0

Dearbhú Cáilíochta agus Cáilíochtaí Éireann
Quality and Qualifications Ireland

PG26320 Postgraduate Diploma in Science in Cybersecurity

Name of Provider	Dublin Business School							
Programme Title	PG26320 Postgraduate Diploma in Science in Cybersecurity							
Award Title	Postgraduate Diploma in Science					**Exit Award Only**	Yes	
Teaching and learning modalities	Lectures / Classes; Practical Sessions; Tutorials							
Delivery Modes	**Award Class**	**Award NFQ Level**	**Award EQF Level**	**Stage**	**Stage NFQ Level**	**Stage Credits**	**First Intake**	**ISCED Code**
Both	Major	9	7	Award Stage	9	60	Sep 2025	06.1.1

Module				**Total Student Effort Module (Hours)**					**Allocation of Marks**				
Title	**Semester**	**Status**	**Credit**	**Total Hours**	**Class Contact Hours**	**Direct e-learning**	**Hours of independent learning**	**Work-based learning efforts**	**C.A. %**	**Project %**	**Skills demonstration %**	**Exam %**	**Workbased %**
Advanced Programming Techniques	1	M	5	125	24	0	101	0	100	0	0	0	0
Advanced Databases	1	M	5	125	24	0	101	0	100	0	0	0	0
Networks and Systems Administration	1	M	5	125	24	0	101	0	100	0	0	0	0
Cryptography & Digital Forensics	1	M	10	250	48	0	202	0	100	0	0	0	0
Cybersecurity Research: Threats, Technologies, and	1	M	5	125	24	0	101	0	100	0	0	0	0
Communications and Networking Security	2	M	10	250	48	0	202	0	100	0	0	0	0
Cybersecurity for Software Development	2	M	5	125	24	0	101	0	100	0	0	0	0
Penetration Testing and Business Continuity Manage	2	M	5	125	24	0	101	0	100	0	0	0	0
Organisational and Societal Cybersecurity	2	M	10	250	48	0	202	0	100	0	0	0	0