



CERTIFICATE OF VALIDATION

New validation

Validation Process: **New**

Provider Name	CCT College Dublin
Date of Validation	21-Sep-23

	Code	Title	Award	Exit Only
Principal Programme	PG25322	Master of Science in Cybersecurity	Master of Science (Masters Degree at NFQ Level 9) 9M22267 90 credits	N/A
Embedded Programme	PG25326	Postgraduate Diploma in Science in Cybersecurity	Postgraduate Diploma in Science (Postgraduate Diploma at NFQ Level 9) 9M22269 60 credits	No

	First Intake	Last Intake
Enrolment Interval	Feb-24	Jan-29

Principal Programme

	Full Time	Part Time	Delivery Mode: full-time / part-time	Full Time, Part Time
Intakes per Annum:	2	2		
Minimum Learners per Intake:	15	15		
Maximum Learners per Intake:	60	60		
Duration (months)	12	18		

Target Learner Groups

The programme is available full-time on-campus and part-time via blended learning mode to both domestic and international applicants. It is designed for graduates of Honours degrees and Higher Diplomas in IT (or cognate disciplines) and IT professionals who are looking to specialise in their studies in order to advance their career as a cybersecurity professional. Strong programming skills is an essential requirement for admission to this programme.

The programme is designed to equip students for roles such as information security analyst, secure application developer, cybersecurity tester, risk advisory on information security and forensics, cloud security analyst.

Brief Synopsis of the Programmes

The Master of Science in Cybersecurity is designed as a specialist postgraduate programme for IT graduates looking to advance their career in the area of cybersecurity. The programme will equip students with advanced knowledge, skill and competence, along with the research capacity, to support them securing leadership roles on graduation. The programme comprises of 60 credits of taught modules and a 30 credit capstone project.

The programme is designed to be a practical in nature with learners required to engage in authentic learning and assessment activities to evidence application of knowledge. In addition to the core technical content, learners will also be exposed to the legal and ethical aspects of cybersecurity.



Minimum Intended Programme Learning Outcomes

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

1. Evidence advanced skills and competence in designing, implementing, and evaluating secure systems and networks based on recent and emerging threats/risk.
2. Undertake research, synthesise and apply knowledge acquired from multiple sources, including academic and professional literature, to inform approaches to real-world scenarios and the development of new technologies and applications.
3. Critically evaluate the impact of different security incidents and breaches on an organisation's reputation and operation; formulate strategies to mitigate the risk, responding to threats, and the normalisation of operations.
4. Evidence expert knowledge of the concepts, theories and practices of current and emerging trends in cybersecurity, including Cryptography, Security Frameworks, Forensic Principles and Analysis, Incident Analysis and Response, and Data and Application Security.
5. Critically evaluate and justify the selection of security policies, procedures and standards (SOC, CSO, GDPR, ISO, NIST, NIS2) and identify potential weaknesses and vulnerabilities based on different security solutions.
6. Work autonomously and collaboratively in leading or contributing to resolving cybersecurity challenges or projects, engaging effectively with all stakeholders.
7. Take responsibility for progressing own learning through critical self-analysis, peer interaction, feedback or input from others, professional development, and undertaking preliminary research.
8. Act with integrity and professionalism, evidencing a sound knowledge of legal, ethical, and data issues related to cybersecurity, and the ability to use this knowledge to determine cybersecurity measures and solutions.
9. Undertake independent research to develop an innovative design of a potential cybersecurity solution, develop and implement this, employing emerging or current industry practice.

Teaching and Learning Modes

1. E-learning (directed)
2. Group Discussions/Interactions
3. Lectures / Classes
4. One-on-One Sessions
5. Other
6. Tutorials
7. Webinars

Approved Countries

Ireland

Physical Resource Requirements

No special resources beyond the existing physical and virtual campus facilities of CCT are required for the delivery of this programme.



Staff Profiles	Qualifications and Experience	WTE
Tech Support	ICT support officers	0.1
Programme Leader	Member of teaching faculty of responsibility for programme management	0.2
Ed Tech	Expertise in using technology to design, create, and deliver curriculum content and learning and assessment activities, employing a variety of tools and platforms, to provide an effective and interactive learning experience in blended learning mode. Works with academic faculty to inform develop, assist in design and creation of content, and undertakes testing as required.	0.25
Lecturer	The CCT policy as approved by QQI, specifies the following: Academic Council of CCT has outlined the minimum requirements for academic appointments as follows: • Evidence of appropriate subject matter expertise is essential, evidenced through academic or professional qualifications, and advanced professional, vocational, technical or research activity in a relevant field. Normally, candidates should have a qualification at the NFQ level above the programme on which they will be teaching. In the case of Masters programmes, a Masters or equivalent professional qualification is normally required. Where potential applicant lecturers do not possess a Masters qualification but are identified as experts in their field, applications should be brought to the attention of the Chair of Academic Council, Dean of Faculty and Dean of Academic Affairs who are authorised to approve a derogation, where deemed appropriate. In such cases, supervision and mentorship in matters relating to teaching and assessment may be required. • Currency of subject matter expertise should be evidenced through recent and regular professional development activity including training and practice. • Training in pedagogy or experience in teaching and assessing is also desirable. Where this is not evidenced, successful candidates will be required to commit to engaging in appropriate activities to develop their experience in this area.	4

Approved Centres	Centre	Minimum Number of Learners per Intake per Centre	Maximum Number of Learners per Intake per Centre
	38484N CCT College Dublin	15	120

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

Learner Teacher Ratios	Learning Activity	Ratio
	Supervision	1:5
	Tutorials	1:20
	Discussion forums and asynchronous learning	1:60
	Live online synchronous classes	1:60
	Group sessions	1:60
	Lectures	1:120



Programme being replaced by this Programme	Prog Code	Programme Title	Validated
	N/A		



Embedded Programme

Validation Process: **New**

Code	Title	Award	Exit Only
PG25326	Postgraduate Diploma in Science in Cybersecurity	Postgraduate Diploma in Science (Postgraduate Diploma at NFQ Level 9) 9M22269 60 credits	No

	Full Time	Part Time	Delivery Mode: full-time / part-time	Full Time, Part Time
Intakes per Annum:	2	2		
Minimum Learners per Intake:	15	15		
Maximum Learners per Intake:	60	60		
Duration (months)	9	12		

Target Learner Groups

The programme is available full-time on-campus and part-time via blended learning mode to both domestic and international applicants. It is designed for graduates of Honours degrees and Higher Diplomas in IT (or cognate disciplines) and IT professionals who are looking to specialise in their studies in order to advance their career as a cybersecurity professional. Strong programming skills is an essential requirement for admission to this programme. This programme is aimed at those potential applicants who want to advance their studies in this area and secure a postgraduate major award without the requirement to undertake a research project. The programme is designed to equip students for roles such as information security analyst, secure application developer, cybersecurity tester, risk advisory on information security and forensics, cloud security analyst.

Brief Synopsis of the Programmes

The Postgraduate Diploma in Science in Cybersecurity is designed as a specialist postgraduate programme for IT graduates looking to advance their career in the area of cybersecurity. The programme comprises of the structured taught component of the MSc and will equip students with advanced knowledge, skill and competence to support them securing leadership roles on graduation. The programme comprises of 60 credits of taught modules and is designed to be practical in nature with learners required to engage in authentic learning and assessment activities to evidence application of knowledge. In addition to the core technical content, learners will also be exposed to the legal and ethical aspects of cybersecurity.

Minimum Intended Programme Learning Outcomes

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

1. Evidence expert knowledge of the concepts, theories and practices of current and emerging trends in cybersecurity, including Cryptography, Security Frameworks, Forensic Principles and Analysis, Incident Analysis and Response, and Data and Application Security.
2. Critically evaluate the impact of different security incidents and breaches on an organisation's reputation and operation; formulate strategies to mitigate the risk, responding to threats, and the normalisation of operations.
3. Undertake research, synthesise and apply knowledge acquired from multiple sources, including academic and professional literature, to inform approaches to real-world scenarios and the development of new technologies and applications.
4. Evidence advanced skills and competence in designing, implementing, and evaluating secure systems and networks based on recent and emerging threats/risk.
5. Critically evaluate and justify the selection of security policies, procedures and standards (SOC, CSO, GDPR, ISO, NIST, NIS2) and identify potential weaknesses and vulnerabilities based on different security solutions.
6. Work autonomously and collaboratively in leading or contributing to resolving cybersecurity challenges or projects, engaging effectively with all stakeholders.
7. Take responsibility for progressing own learning through critical self-analysis, peer interaction, feedback or input from others, professional development, and undertaking preliminary research.
8. Act with integrity and professionalism, evidencing a sound knowledge of legal, ethical, and data issues related to cybersecurity, and the ability to use this knowledge to determine cybersecurity measures and solutions.



Teaching and Learning Modes	1. Directed Learning 2. E-learning (directed) 3. Group Discussions/Interactions 4. Lectures / Classes 5. Tutorials 6. Webinars
------------------------------------	---

Approved Countries	Ireland
---------------------------	---------

Physical Resource Requirements

No special resources beyond the existing physical and virtual campus facilities of CCT are required for the delivery of this programme.

Staff Profiles	Qualifications and Experience	WTE
Lecturer	The CCT policy as approved by QQI, specifies the following: Academic Council of CCT has outlined the minimum requirements for academic appointments as follows: • Evidence of appropriate subject matter expertise is essential, evidenced through academic or professional qualifications, and advanced professional, vocational, technical or research activity in a relevant field. Normally, candidates should have a qualification at the NFQ level above the programme on which they will be teaching. In the case of Masters programmes, a Masters or equivalent professional qualification is normally required. Where potential applicant lecturers do not possess a Masters qualification but are identified as experts in their field, applications should be brought to the attention of the Chair of Academic Council, Dean of Faculty and Dean of Academic Affairs who are authorised to approve a derogation, where deemed appropriate. In such cases, supervision and mentorship in matters relating to teaching and assessment may be required. • Currency of subject matter expertise should be evidenced through recent and regular professional development activity including training and practice. • Training in pedagogy or experience in teaching and assessing is also desirable. Where this is not evidenced, successful candidates will be required to commit to engaging in appropriate activities to develop their experience in this area.	3
Ed Tech	Expertise in using technology to design, create, and deliver curriculum content and learning and assessment activities, employing a variety of tools and platforms, to provide an effective and interactive learning experience in blended learning mode. Works with academic faculty to inform develop, assist in design and creation of content, and undertakes testing as required.	0.25
Programme Leader	Member of teaching faculty of responsibility for programme management	0.2
Tech Support	IT Support Officers	0.1

Approved Centres	Centre	Minimum Number of Learners per Intake per Centre	Maximum Number of Learners per Intake per Centre
	38484N CCT College Dublin	15	120



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

Learner Teacher Ratios	Learning Activity	Ratio
	Lectures	1:120
	Group sessions	1:60
	live online synchronous classes	1:60
	discussion forums and asynchronous learning	1:60
	tutorials	1:20

Programme being replaced by this Programme	Prog Code	Programme Title	Validated
	N/A		



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 writing, 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 certification.

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

1.

Part 2.5 Special Conditions of Validation



Programme and stage schedules

PG25322 Master of Science in Cybersecurity

Name of Provider		CCT College Dublin													
Programme Title		PG25322 Master of Science in Cybersecurity													
Award Title		Master of Science							Exit Award Only		N/A				
Teaching and learning modalities		E-learning (directed); Group Discussions/Interactions; Lectures / Classes; One-on-One Sessions; Other; Tutorials; Webinars													
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		Feb 2024			06.1.2		
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 %
Cryptography Theory and Practice			1	M	5	125	30	0	95	0	100	0	0	0	0
Security Frameworks and Compliance			1	M	5	125	30	0	95	0	100	0	0	0	0
Secure Programming and Scripting			1	M	10	250	60	0	190	0	100	0	0	0	0
Forensic Principles and Analysis			1	M	10	250	60	0	190	0	100	0	0	0	0
Data and Application Security			2	M	10	250	60	0	190	0	100	0	0	0	0
Research and Professional Ethics			2	M	5	125	30	0	95	0	100	0	0	0	0
Penetration Testing and Malware Analysis			2	M	10	250	60	0	190	0	100	0	0	0	0
Incident Analysis and Response			2	M	5	125	30	0	95	0	100	0	0	0	0
Capstone Project			3	M	30	750	20	10	720	0	0	100	0	0	0



PG25326 Postgraduate Diploma in Science in Cybersecurity

Name of Provider		CCT College Dublin													
Programme Title		PG25326 Postgraduate Diploma in Science in Cybersecurity													
Award Title		Postgraduate Diploma in Science							Exit Award Only		No				
Teaching and learning modalities		Directed Learning; E-learning (directed); Group Discussions/Interactions; Lectures / Classes; Tutorials; Webinars													
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		Feb 2024		06.1.2		
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 %
Cryptography Theory and Practice			1	M	5	125	30	0	95	0	100	0	0	0	0
Security Frameworks and Compliance			1	M	5	125	30	0	95	0	100	0	0	0	0
Secure Programming and Scripting			1	M	10	250	60	0	190	0	100	0	0	0	0
Forensic Principles and Analysis			1	M	10	250	60	0	190	0	100	0	0	0	0
Data and Application Security			2	M	10	250	60	0	190	0	100	0	0	0	0
Research and Professional Ethics			2	M	5	125	30	0	95	0	100	0	0	0	0
Penetration Testing and Malware Analysis			2	M	10	250	60	0	190	0	100	0	0	0	0
Incident Analysis and Response			2	M	5	125	30	0	95	0	100	0	0	0	0