QQI
Quality and Qualifications Ireland
Dearbhú Cáilíochta agus Cáilíochtaí Éireann

Report of the Programme Evaluation Panel

Provider's Name:	National College of Ireland
Address:	Mayor Square, IFSC Dublin 1
QA procedures agreed on:	2006
QA procedures reviewed on:	2010
Programme(s) submitted for approval:	**Leading to the award of:**
1. MSc in Cybersecurity	Master of Science
2. Postgraduate Diploma in Science in Cybersecurity	Postgraduate Diploma in Science
Date submitted to QQI:	11th April 2016
Date of Evaluation:	10th May 2016
Date of Report:	11th May 2016

Membership of the Programme Evaluation Panel:

Role	Name	Area of Expertise	QQI Peer Review Reference Listing
Chairperson	Dr Joseph Ryan	QA/Learning & Teaching	
External Specialist	Dr Fredrick Mtenzi	Cybersecurity	
External Specialist	Mr Stephen Sheridan	Cybersecurity	
Industry/Employer Perspective	Mr Chris Patterson*	Cybersecurity	
Rapporteur	Sinéad O'Sullivan		

Mr Patterson was unavoidably detained on the morning of the panel due to a family emergency.

QQI
Quality and Qualifications Ireland
Dearbhú Cáilíochta agus Cáilíochtaí Éireann

1 Profile of provider:

The National College of Ireland (NCI) has an immensely proud history as a third level educational institution. Established by the Jesuit order in 1951 as the Catholic Workers College it quickly gained recognition for excellence in its subject fields, particularly human resource management and industrial relations, and for the provision of high quality educational opportunities for employees entering third level education. In the late 1990's the College became the National College of Ireland and entered a new phase of its development expanding its part-time provision to a number of off-campus locations throughout the country and extending its full-time undergraduate programmes to include accountancy, finance and informatics. In 2002 the College moved from its original site in Ranelagh to a new 'State of the Art' purpose built premises in Dublin's International Financial Services Centre.

NCI's educational philosophy and operational structure embody participation, collaboration and applied problem solving strategies. These are enabled by a faculty whose qualifications and professional experience help integrate academic theory with current practical application. The College assesses both the quality of its academic programmes and the academic achievement of its students and utilises the results of these assessments to improve academic and institutional quality.

The primary focus of NCI is on maintaining a centre of excellence that is centred on the changing needs of today's learner. National College of Ireland provides a broad range of high-quality education programmes for today's knowledge-based society.

In line with its mission of widening access to education, the College places a strong emphasis on the needs of the learner, bringing a unique student-centred approach to all aspects of its teaching and research. National College of Ireland provides a range of learning options that extend beyond traditional classroom dynamics, including distance learning and internet-based learning programmes

2 Planning:

The College has developed a significant number of programmes since its last institutional review culminating in 2015 with a complete programmatic review of its portfolio across the Business, Computing and Education subject areas.

2.1 Purpose of the award

The aim of this programme is to provide learners with essential research and expert technical knowledge and competence of the most important technical concepts of security applied in emerging technologies such as cloud, mobile, Internet of Things and big data storage systems.

The course is practical in nature and develops in-depth expertise of core technical topics such as cryptography, forensic investigation, network security, development of secure application, malware

analysis, and technologies and tools that support application and service vulnerability detection, incident detection, data and log retrieval and analysis. Supplementary to the core technical competencies, learners will have exposure to IT law and ethics associated with the security domain.

Does the proposed programme address a clear market demand? Yes✓ No

2.2 Avoidance of duplication

Has the Programme Development Team identified the availability of similar programmes locally, regionally, nationally?

Yes✓ No

Comment: None

2.3 Stakeholder consultation

Was the level of stakeholder engagement satisfactory? Yes✓ No

See below

Support for the programme (industry/business/community) Yes✓ No

There has been significant industry consultation and support throughout the development and validation process of this programme.

2.4 Efficient and effective use of resources

Does the proposed programme represent both efficient and effective use of the provider's resources?

Yes✓ No

Comment: None

2.5 Resource development over last 5 years (or in direct support of this programme)

Specific Comments:

Staff:
The panel notes that the College has indicated that it is currently recruiting full-time faculty. Whilst recognising the advantages of having industry based teaching staff on the programme, the panel conditions that at least one of the faculty being recruited in the current cycle holds a specialism in Cybersecurity in order to support the programme as committed to by management during the meeting.

Accommodation: The panel is satisfied that the accommodation required to deliver the programme is available to the programme.

Information technology: The panel is satisfied that the ICT required to deliver the programme is available to the programme

Library: The panel is satisfied that the library & information service required to deliver the programme is available to the programme

Administration: The panel is satisfied that the administration and programme organisation structures required to deliver the programme are available to the programme

Publicity/public information: The panel is satisfied that the appropriate information will be made available to learners in relation to entry requirements, award and regulations of the programme.

2.6 Planned development over the coming 5 years?

Have the QQI award standards been explicitly referred to in the programme and does the programme meet those standards at the specified level?

Yes No✓

Comment: None

Has the Provider complied with Protection for Enrolled Learner requirements?

Yes No✓

The panel understands that PEL requirements for any learners recruited under HEA labour activation schemes will be provided by the HEA. Otherwise PEL will be provided under an arrangement with HECA which is currently being finalised and will be made available to QQI prior to the enrolment of any learner.

2.7 Access

Is the expected minimum and maximum number of all learners entering the programme explicitly stated?

Yes✓ No

Comment: None

Have any/all prerequisite knowledge, skills or competence or any other specific entry requirement been articulated?

Yes✓ No

The panel notes that the entry requirements for the programme are outlined. However, the expectation of the abilities of learners with respect to programming and mathematical abilities should be clearly articulated.

3 Quality Assurance

3.1 Application of agreed quality assurance procedures for development of programmes

Were the agreed quality assurance procedures for programme development followed?

Yes✓ No

Has the programme team demonstrated how programme delivery will be monitored in accordance with agreed QA procedures?

Yes✓ No

The Domain Context and Internship modules bring particular challenges to the quality assurance of the programme. The panel is satisfied that the College and Programme Team are aware of and have the processes in place to ensure consistency in the treatment of learners and that there is clarity regarding the role of the College and potential employer or host company with respect to assessment and intellectual property.

The panel recommends the explicit inclusion of an employer host induction briefing day which outlines the roles and responsibilities of each stakeholder in the process.

Are programme management arrangements adequate and coherent?

Yes✓ No

A programme director (Academic) and programme co-ordinator (administrative) will be assigned to the programme.

4 Programme structure and content

Is the programme structure well designed, coherent and fit for its stated purpose

Yes No✓

[redacted] More emphasis should be made on security at the design stage of an application rather than its remedy after a breach.

4.1 Programme learning outcomes

Do the programme learning outcomes comply with national standards for the level of award proposed?

Yes✓ No

While the programme learning outcomes have been mapped to the level 9 Science standards, the panel conditions the programme team to clearly state the programme learning outcomes in a single list and to ensure that they reflect a level 9 set of outcomes in all cases.

Are module descriptions adequate and relevant? Yes No✓

The indicative curriculum of each of the modules is well defined, however, more detail and more articulation of teaching and assessment strategies is required for all modules. Care should be taken to ensure that there is a consistency of curriculum outlined, in particular for 5 credit modules.

Are modules relevant and current? Yes✓ No

Comment: None

Does the combination of modules chosen have the coherence to support the proposed award?

Yes✓ No

As noted above, the panel is of the view that the structure should be reviewed to ensure that it is focussed and integrated. The team should review again, the balance of 5 and 10 credit modules and ensure any unessential overlap is minimised.

4.2 Learning Modes ✓

Can the teaching and learning strategies proposed support achievement of the required learning outcomes?

Yes✓ No

Whilst the document outlined various methods by which modules could be taught, the panel conditions that these are more specific both at a programme and modular level with differentiated approaches taken as appropriate to the modules.

Are the delivery mechanisms proposed adequate to the needs of the programme and the proposed learner cohorts?

Yes✓ No

Comment: None

4. Assessment strategies

Are assessment processes and methods adequately described? Yes No✓

The assessment regulations for the programme are clearly outlined in the programme documentation and these follow guidelines for Assessment Standards.

As with the teaching and learning strategies, more detail is required at a modular level to ensure that it is clear what is expected of the learner and that the assessment is at the appropriate level.

Are these strategies appropriate to this type of award, in terms of type, frequency and volume?

Yes No✓

Is assessment explicitly linked with intended learning outcomes? Yes✓ No

Does the assessment strategy underpin the achievement of the relevant standard of knowledge, skill and competence?

Yes No✓

In relation to the above questions, the lack of specificity of assessment approach to be used has made it difficult for the panel to be definitive in its response. The panel is satisfied that the intent is in place, however, some of the sample assessments indicated did not demonstrate and expectation of level 9 standards.

4.4 Duration

What is the intended duration of the Programme?

MSc in Cybersecurity: 1 calendar year full-time, 2 calendar years part-time.
The panel recommends consideration of extending the write up component of the internship beyond the completion of the internship which will extend the full-time duration.

Postgraduate Diploma in Science in Cybersecurity: 1 academic year full-time, 2 academic years part-time

What is the lifespan of the programme (e.g. single cohort intake to satisfy limited local demand; multiple intakes over the following 5 years etc.?)

The programme team has outlined an intake per academic year over the next 5 years.

Does the Panel believe this to be realistic? Yes✓ No

The panel advises caution in terms of the scalability of the programme to ensure that elements of the programme such as the internship and domain context modules are sufficiently bedded down

Are there flexible modes of participation? Yes✓ No

4.5 Credits

Is credit allocation in accordance with national and international guidelines?

Comment: None

Yes✓ No

Considering the level, outcomes and volume of each module, is the number of credits attached to each appropriate?

Yes✓ No

The team should review again, the splitting of modules into 5 credit modules and ensure any unessential overlap is minimised and the balance of content is consistent across modules

Considering the stated objective of the programme is the number of credits attached to the award appropriate?

Yes✓ No

Comment: None

4.6 NFQ Level

Is the proposed level of the programme in accordance with institutional policy/national norms?

Yes✓ No

Comment: None

4.7 Programme titles and award

Is the title consistent with national policy, is it informative and is it fit for purpose?

Yes✓ No

Comment: None

4.8 Transfer and Progression

Has the Programme Development Team identified realistic transfer and progression opportunities/possibilities that learners may avail of following achievement of this award?

Yes✓ No

The panel notes the inclusion of documentation for a Postgraduate Diploma in Science in Cybersecurity which is proposed as both an ab initio award and a transfer mechanism for learners who do not or cannot complete the Internship and Domain Context modules. This needs to be described clearly and as an independent award.

QQI
Quality and Qualifications Ireland
Dearbhú Cáilíochta agus Cáilíochtaí Éireann

5 Module Titles, Content and Assessment Strategy

 od les . – 5.10 are offered on the Postgraduate Diploma in Science in Cybersecurity only. Modules 5.1 – 5.14 are offered on the MSc in Cybersecurity.

5.1 Security Fundamentals

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓ No

Comment: None

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes No✓

The module teaching, learning and assessment strategies should be reviewed to ensure that a specific strategy is chosen, is clear to anyone reading the descriptor and that the assessment instrument is appropriate to the module learning outcomes. The sample assessments provided should be appropriate to the level of the programme.

Is the required reading and supplementary reading appropriate, current and realistic?

Yes✓ No

5.2 Secure Programming 1

Is the title informative and is it fit for purpose? Yes✓ No

The panel recommends consideration of 'Secure Programming for the Web' as this reflects the content

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓ No

The module content is significantly more detailed in this module than in other 5 credit modules. This should be reviewed to ensure that an appropriate balance is maintained.

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes No✓

The module teaching, learning and assessment strategies should be reviewed to ensure that a specific strategy is chosen, is clear to anyone reading the descriptor and that the assessment instrument is appropriate to the module learning outcomes. The sample assessments provided should be appropriate to the level of the programme.

Is the required reading and supplementary reading appropriate, current and realistic?

Yes✓ No

Comment: None

5.3 Cryptography

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓ No

Comment: None

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes No✓

The module teaching, learning and assessment strategies should be reviewed to ensure that a specific strategy is chosen, is clear to anyone reading the descriptor and that the assessment instrument is appropriate to the module learning outcomes. The sample assessments provided should be appropriate to the level of the programme.

Is the required reading and supplementary reading appropriate, current and realistic?

Yes✓ No

Comment: None

5.4 IT Law & Ethics

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓ No

Comment: None

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes No✓

The module teaching, learning and assessment strategies should be reviewed to ensure that a specific strategy is chosen, is clear to anyone reading the descriptor and that the assessment instrument is appropriate to the module learning outcomes. The sample assessments provided should be appropriate to the level of the programme.

The balance of assessment afforded to □earning □utcome □should be reviewed.
There is an opportunity to consider some integration of assessment with the □orensics □ e□iscovery module. Notwithstanding that these are planned to be delivered in a different semester, the same case or context could be used in order to integrate concepts

Is the required reading and supplementary reading appropriate, current and realistic?
Yes✓ No

Comment: None

5.5 Network Security

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓ No

The description of the content of this module should be expanded so that the intent of coverage and context is clear to any reader e.g. ‘footprinting’, ‘scanning’ etc. The objectives of the module should be made more specific.

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes No✓

The module teaching, learning and assessment strategies should be reviewed to ensure that a specific strategy is chosen, is clear to anyone reading the descriptor and that the assessment instrument is appropriate to the module learning outcomes. The sample assessments provided should be appropriate to the level of the programme.

Is the required reading and supplementary reading appropriate, current and realistic?
Yes✓ No

□omment□None

5.6 Forensics & eDiscovery

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓ No
.
Comment: None

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes No✓

The module teaching, learning and assessment strategies should be reviewed to ensure that a specific strategy is chosen, is clear to anyone reading the descriptor and that the assessment instrument is appropriate to the module learning outcomes. The sample assessments provided should be appropriate to the level of the programme.
There is an opportunity to consider some integration of assessment with the IT & Ethics module. Notwithstanding that these are planned to be delivered in a different semester, the same case or context could be used in order to integrate concepts.

Is the required reading and supplementary reading appropriate, current and realistic?
Yes✓ No

Comment: None

5.7 Research in Computing

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Comment: None

Yes✓ No

Is the content sufficiently informative and is it fit for purpose? Yes✓ No
.
Comment: None

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes✓ No

□s noted by the programme team, the assessment brea□down should be amended to reflect the actuality of delivery which is □□□ for the research □uestion and □□□ for the □iterature□roposal.

Is the required reading and supplementary reading appropriate, current and realistic?
Yes✓ No

Comment: None

5.□ Secure Programming 2

Is the title informative and is it fit for purpose? Yes✓ No

□s with □ecure □rogramming □, the panel recommends consideration of *Secure Programming for Application Development.*

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓ No
.
Comment: None

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes No✓

The module teaching, learning and assessment strategies should be reviewed to ensure that a specific strategy is chosen, is clear to anyone reading the descriptor and that the assessment instrument is appropriate to the module learning outcomes. The sample assessments provided should be appropriate to the level of the programme.

Is the required reading and supplementary reading appropriate, current and realistic?
Yes✓ No

Comment: None

5.□ Web Application Security

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓ No

.
This content should be reviewed to ensure that any overlap with □ecure □rogramming □& □is removed. The inclusion of security of the browser in use should be explicitly included.

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes No✓

The module teaching, learning and assessment strategies should be reviewed to ensure that a specific strategy is chosen, is clear to anyone reading the descriptor and that the assessment instrument is appropriate to the module learning outcomes. The sample assessments provided should be appropriate to the level of the programme.

Is the required reading and supplementary reading appropriate, current and realistic?

Yes✓ No

Comment: None

5.□□ Incident Response & Analytics

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes No✓

.
The security context of the module should be explicitly referenced in the curriculum outline and the curriculum should be expanded beyond the current high level outline.

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes No✓

The module teaching, learning and assessment strategies should be reviewed to ensure that a specific strategy is chosen, is clear to anyone reading the descriptor and that the assessment instrument is appropriate to the module learning outcomes. The sample assessments provided should be appropriate to the level of the programme.

Is the required reading and supplementary reading appropriate, current and realistic?

Yes✓ No

Comment: None

5. Malware Analysis

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓ No

.

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes No✓

The module teaching, learning and assessment strategies should be reviewed to ensure that a specific strategy is chosen, is clear to anyone reading the descriptor and that the assessment instrument is appropriate to the module learning outcomes. The sample assessments provided should be appropriate to the level of the programme.

Is the required reading and supplementary reading appropriate, current and realistic?
Yes✓ No

Comment: None

5. Domain Context

Is the title informative and is it fit for purpose? Yes✓ No

[illegible]

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓ No

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Comment: None

Yes✓ No

Is the required reading and supplementary reading appropriate, current and realistic?

Yes✓ No

Comment: None

5.□□ Research Methods

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

Comment: None

Is the content sufficiently informative and is it fit for purpose? Yes✓□ No
Comment: None

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Comment: None

Yes✓ No

Is the required reading and supplementary reading appropriate, current and realistic?
Yes✓ No

Comment: None

5.□□ Internship

Is the title informative and is it fit for purpose? Yes✓ No

Comment: None

Are the specific learning outcomes a) properly stated, b) sufficient and c) achievable?

Yes✓ No

The learning outcomes should be reviewed to ensure that the taxonomy used is consistently at level 9.

Is the content sufficiently informative and is it fit for purpose? Yes✓□ No

The description of the contract paragraph should be extended to include information on how intellectual property and data privacy issues will be handled.

Does the Assessment Strategy align sufficiently with the intended learning outcomes?

Yes✓ No

The panel is of the view that the write up period for the internship should be consecutive rather than concurrent with the internship and thus ma□ing the internship process last over a longer period.

Is the required reading and supplementary reading appropriate, current and realistic?
Yes✓ No

Comment: None

6 Specific Issues to be addressed by the provider

The panel re□uires resubmission of documentation for both awards addressing the following:

□.□ Conditions of Approval:

C1. The College must follow through on its commitment to recruit a specialist in Cybersecurity
C2. The programme learning outcomes should be listed separately to the mapping provided in section 6 of the documentation
C3. The programme content should be reviewed to ensure that academic priorities take precedence over industry led priorities and a narrower focus should be taken. The creation of a graduate profile may assist in creating that focus.
C4. Programme and module learning outcomes should be reviewed to ensure that the taxonomy used consistently represents level 9 on the National Framework of Qualifications
C5. The entry requirements of the programme should clearly set expectations with respect to mathematical and programming ability
C6. The module learning, teaching and assessment strategies should be specific to each module
C7. The write up period from the Internship module should be made consecutive to the internship period itself
C8. In order to ensure consistency and continuity, a 'company preparation' day should be set up to brief companies on their role and responsibilities with regard to the Domain Context and Internship modules

6.2 Recommendations:

R1. Consider changing the titles of Secure Programming 1 & 2 to Secure Programming for the Web and Secure Programming for application development
R2. Include the security of the browser within the Web Application Security module
R3. The concept of 'Security in Design' should be brought more to the fore
R4. The language used in the module curricula should be made specific to the security context for the avoidance of doubt and expanded where outlined in section 5 above.
R5. The intake of the programme should be closely monitored particularly in the early years in order to ensure its scalability

QQI
Quality and Qualifications Ireland
Dearbhú Cáilíochta agus Cáilíochtaí Éireann

1. Overall Result of Evaluation Panel Review:

The Programme is recommended to the Programmes and Awards Executive Committee for approval subject to the provision to QQI of a revised submission document including programme schedule(s), which addresses the conditions and recommendations required in the report and which has been signed off by the Panel Chair if necessary.

This report has been agreed by the Evaluation Panel and is signed on their behalf by the Chair.

Panel Chairperson: Dr Joseph Ryan Date: 25th May 2016

Signed _ Date _

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.

QQI
Quality and Qualifications Ireland
Dearbhú Cáilíochta agus Cáilíochtaí Éireann

Appendix 1: Staff

Staff Name	Role
Dr Phillip Matthews	President
Prof Jimmy Hill	Vice President Academic & Admin
Mr John McGarrigle	Registrar
Dr Pramod Pathak	Dean School of Business
Dr Cristina Hava Muntean	Programme Director
Dr Paul Stynes	Vice Dean, School of Computing
Dr Simon Caton	School of Computing
Mr Michael Bradford	School of Computing
Mr Vikas Sahni	School of Computing
Mr Fabio Cerullo	School of Computing
Dr Arlene Egan	NCI Learning & Teaching
Ms Frances Sheridan	School of Computing
Dr Maria Moloney	School of Computing
Mr Owen Pendlebury	School of Computing
Ms Karen Murray	Lecturer, Law, School of Business
Ms Caroline Kennedy	Careers & Employability Office
Ms Sinéad O'Sullivan	Director of Quality Assurance & Statistical Services

National College of Ireland

MSc in Cyber Security
Postgraduate Diploma in Science in Cyber Security

New Programme Validation

Programme Team Response

The programme team for the MSc/Postgraduate Diploma in Science in Cyber Security programme would like to express their appreciation of the Expert Panel's deliberations and feedback.

The programme presented to the External Panel has undergone a set of considered amendments based on the panel's feedback and the conditions and recommendations relating to the proposed programme as outlined below.

MSc in Cyber Security

Conditions

Condition	Response
C□□ The College must follow through on its commitment to recruit a specialist in Cybersecurity	NCI is currently in the process of recruiting a faculty member to satisfy the condition of running an MSc in Cyber Security□
C□□ The programme learning outcomes should be listed separately to the mapping provided in section □ of the documentation	Section □□□□ Minimum Intended Programme Learning Outcomes & Award Standards was revised□ Eight Minimum Intended Programme Learning Outcomes □MIPLO□were defined and ensured that the ta□onomy is consistent with the level of the programme as prescribed by the QQI award standards for Computing at level □□ Table □ was also updated to indicate the mapping of the eight MIPLOs into the modules learning outcomes□
C□□ The programme content should be reviewed to ensure that academic priorities take precedence over industry led priorities and a narrower focus should be taken□ The creation of a graduate profile may assist in creating that focus□	Academic staff are assigned for all modules defined in the programme and they have addressed and implemented the panel's recommanded changes (e.g module's learning outcomes appropriate for level 9, module teaching and learning startegy specific to the module, module assessment strategy and detail sample assessments for each module) The structure of the programme was also changed to address panel recommendations in terms of having a narrower focus. Therefore two specialisations have been introduced: Forensics and Cloud Security. Each specialisation has 15 credits allocated and aims to provide a narrower focus into a specific context where security principles are applied. The whole programme document (e.g. Introduction, Proposed programme schedule,

Condition	Response
	Programme aim, Programme ob□ectives, Programme learning outcomes etc.) was updated to reflect the new structure and the two specialisations. □ new section □.1.□ Programme Specialisations was introduced. □ new module named Cloud Security (1□ credits, elective) was introduced into the programme.
C□. Programme and module learning outcomes should be reviewed to ensure that the taxonomy used consistently represents level 9 on the □ational Framewor□ of □ualifications	The following eight □inimum Intended Programme □earning □utcomes (□IP□□s) have been defined: • □IP□□1: Compare and contrast technical concepts of security, technologies and tools that support secure application development, application and service vulnerability detection and patching, data and logs retrieval and analysis. • □IP□□□: □esearch by applying standard and customised research methodologies and critically, analyse, evaluate and synthesise original wor□s in a number of cutting□edge Cyber Security topics. • □IP□□□: Communicate effectively to a range of audiences in both written and verbal media • □IP□□□: □tilise practical s□ills, technologies and tools that support secure programming, application and service vulnerability detection and patching, cryptanalysis, security incidents detection and log file analysis. • □IP□□5: Integrate technologies and security concepts to solve a challenging Cyber Security problem and to successfully plan, develop and test a security product within a given context (e.g. cloud security and forensics). • □IP□□□: □a□e decisions and address security re□uirements through analytical thin□ing, communication and interaction • □IP□□□: □nalyse, identify and document measures to address vulnerabilities, ris□s, wea□nesses, and other safety aspects relevant to computing systems within a given context (e.g. cloud security and forensics) • □IP□□□: Identify □nowledge gaps and

Condition	Response
	underta□e self□learning to ac□uire new □nowledge and meet the re□uirements of the rapidly developing and expanding security industry. The learning outcomes of all modules have been revised to ensure that the taxonomy used is apprpriate for a level 9 degree. The following module learning outcomes have been revised: • Security Fundamentals: □□1, □□5 • Cryptography: □□1, □□□, □□□ • IT □aw and Ethics: □□5 • □alware □nalysis: □□□ • Incident □esponse □ □nalytics: □□1, □□□ • □esearch □ethods: □□5 • Secure Programming for □pplication □evelopment: □□1
C5. The entry re□uirements of the programme should clearly set expectations with respect to mathematical and programming ability	The □inumum □cademic □e□uirements of the programme (see Section □) have been updated and they clearly set the expectations with respect to programming ability. *"An honours (level 8) primary degree in Computing or a cognate area with a 2.2 award or higher. Candidates are expected to have programming ability* *Cognate area means a STEM (Science, Technology, Engineering, and Mathematics) degree that also taught programming/application development related modules*." The paragraph related to □PE□ assessment was also updated and it clearly set that the programming ability of the applicant will be assessed. The programme team has decided that there is no special re□uirement regarding the mathematical ability apart of the mathematical s□ills gain from a □evel □ degree in Computing or cognate area. Cognate area means a STE□ (Science, Technology, Engineering, and □athematics) degree. This is because the Cryptography module decriptor was updated. □ore specific, the module ob□ectives section indicates now that an overview of core mathematical concepts is also provided so that learners may effectively engage with the content. □athematical Preliminaries topic was also added to the module curriculum.
C□. The module learning, teaching and assessment strategies should be specific to	□ll module descriptors have been revised in

Condition	Response
each module	terms of: - Teaching and Learning Strategy has been updated to reflect actual practice to be applied for each module. - Assessment Strategy clearly indicates the assessment type, the assessment weight, appropriate assessment description and the module's learning outcomes assessed. - Sample Assessments section provides actual project description, tasks, essay or questions that can be given in the assignments. The module learning outcomes assessed by each sample assessment is also indicated.
C7. The write up period from the Internship module should be made consecutive to the internship period itself	The Internship module decriptor (Module Curriculum section) clearly specify now that extra time is provided for writing the required assessment documents and for the preparation of the viva (presentation) after the completion of the work within the company enviroment. *"The internship runs over 15 weeks, in the last semester of the programme. It requires working full-time for the first 12 weeks in an ICT related business environment. The last 3 weeks will be allocated for the preparation of the portfolio to be submitted and viva"* The above parapraph was also included in Section 4.6.4 Management of the Internship to clearly indicate the new duration of the Internship module.
C8. In order to ensure consistency and continuity, a 'company preparation' day should be set up to brief companies on their role and responsibilities with regard to the Domain Context and Internship modules	The Domain Context module decriptor was updated to include a detail Operational Plan (section 5.9.3). It clearly indicates the engagement process between the academic staff and the company facilitators and the mechanism to be applied to ensure that the academic standards are followed in the teaching and assessment process of the module.

National College of Ireland

Recommendations

Recommendation	Response
R1. Consider changing the titles of Secure Programming 1 & 2 to Secure Programming for the Web and Secure Programming for application development	Secure Programming 1 and Web Application Security were merged and expanded to 10 credits in order to remove the topics overlap that existed between the two modules and to ensure a more detailed focus on Web Security aspects is provided. The new 10 credits module that was created was named Secure Programming for Web. Secure Programming 2 was retitled as Secure Programming for Application Development. A new topic on Principles of Secure Design (15%) was also added to the module curriculum.
R2. Include the security of the browser within the Web Application Security module	Browser Security Model (10%) topic was added into the module curriculum section of the Secure Programming for Web module.
R3. The concept of 'Security in Design' should be brought more to the fore	A new topic on Principles of Secure Design (15%) was added into the module curriculum section of the Secure Programming for Application Development module.
R4. The language used in the module curricula should be made specific to the security context for the avoidance of doubt and expanded where outlined in section 5 above.	Detail sample assessments are provided now for all modules. These sample assessments clearly indicate that the topics delivered by a specific module are assessed in the security context.
R5. The intake of the programme should be closely monitored particularly in the early years in order to ensure its scalability	The figures on the predicted maximum number of students to be enrolled into the programme over the next 4 years, presented in section 3 Outline of the Proposed Programme have been reduced as following: Year 1: from 50 to 30 students Year 2: from 60 to 40 students Year 3: from 65 to 50 students Year 3: from 75 to 60 students This plan will double the students number in four years' time.

In addition the following changes have been implemented:

- The individual comments indicated for each module in the QQI Panel Report - Section 5 Module titles, Content and Assessment Strategy have also been addressed.
- Two specialisations named Forensics and Cloud Security were introduced in the programme structure.
- A new module named Cloud Security, 10 credits, elective and available only with the Cloud Security specialisation was introduced.
- Forensics and eDiscovery module was changed from mandatory into an elective module available only with the Forensics specialisation.

- Incident Response and Analytics module was changed from mandatory into an elective module available only with the Forensics specialisation
- Domain Context module is elective within each specialisation. Different instances of the module specific to the specialisation may be run.
- □etwork Security module was retitled as □etwork Security and Penetration Testing. Some topics related to penetration testing were introduced into the module curriculum. □O1 was also introduced to reflect the penetration testing concepts introduced by the module.

National College of Ireland

Postgraduate Diploma in Science in Cyber Security

□□e di□□e□ences t□at e□ist □et□een t□e t□o doc□ments c□eated □o□t□e □□c in □□□e□ □ec□□it□ and □ost□□ad□ate □ip□oma in □□□e□ □ec□□it□ p□o□□ammes a□e □isted □e□o□□

□□e p□o□□amme p□oposed st□□ct□□e is di□□e□ent□
□□e □ost□□ad□ate □ip□oma is a □□ c□edits co□□se □□i□e t□e □aste□s co□□se is □□ c□edits□□□e □aste□s co□□se □as □ e□t□a mod□□es□ Resea□c□ □et□ods □□ c□edit□ and □nte□ns□ip □□□ c□edits□□

□□e □inim□m □ntended □□o□□amme □ea□nin□ □□tcomes □□ □□□□ □□o□t□e t□o p□o□□ammes a□e di□□e□ent□□□e post□□ad□ate dip□oma □as □ □□□□□s □isted □e□o□□

- □ □□□□ □□□emonst□ate an a□a□eness and c□itica□□nde□standin□ o□sec□□it□ concepts□ tec□no□o□ies and too□s t□at s□ppo□t sec□□e app□ication de□e□opment□app□ication and se□□ice □□□me□a□i□t□ detection and patc□in□□data and □o□s □et□ie□a□and ana□□sis
- □ □□□□ □□ □□itica□□□ assess and app□aise t□e scienti□c □o□□ in a n□m□e□ o□ c□ttin□□ ed□e □□□e□□ec□□it□topics
- □ □□□□ □□ □omm□nicate to a □an□e o□ a□diences in □ot□ □□itten and □e□a□media a□o□t t□e eme□□in□ t□eo□ies and tec□no□o□ies in an a□tic□□ate and con□incin□ □as□ion
- □ □□□□ □□ □ti□se p□actica□ s□i□s□ tec□no□o□ies and too□s t□at s□ppo□t sec□□e p□o□□ammin□□ app□ication and se□□ice □□□me□a□i□t□ detection and patc□in□□ c□□ptana□□sis□sec□□it□ incidents detection and □o□ □i□e ana□□sis
- □ □□□□ □□ □nte□□ate tec□no□o□ies and sec□□it□ concepts to so□□e a c□a□□en□in□ □□□e□ □ec□□it□ p□o□□em and to s□ccess□□□□ p□an□de□e□op and test a sec□□it□ p□od□ct □it□in a □i□en conte□t e□□□□c□o□d comp□tin□ o□□o□ensics□□
- □ □□□□ □□ □na□□se□identi□□ and doc□ment meas□□es to add□ess □□me□a□i□ties□□is□s□ □ea□nesses□and ot□e□ sa□et□ aspects □e□e□ant to comp□tin□ s□stems □it□in a □i□en conte□t e□□□□c□o□d comp□tin□□o□□o□ensics□
- □ □□□□ □□ □ndependent□□ ac□□i□e and assess □no□□d□e in ne□ and eme□□in□ tec□no□o□ies □om t□e c□□e□sec□□it□domain□

□□e □□o□□amme o□□ecti□es a□e □a□e □een di□□e□entiated □o□t□e t□o p□o□□ammes□

□□e emp□asis on de□e□opin□ □esea□c□ s□i□s is □ed□ced in t□e □□ □ip□oma compa□ed to t□e □aste□s co□□se d□e to t□e □ mod□□es □□□ c□edits in tota□□□esea□c□ □e□ated t□at e□ist on□□ in t□e □aste□s p□o□□amme□

□□□ t□e mod□□e □e□ated c□an□es □ecommended and imp□emented □o□ t□e □□c in □□□e□ □ec□□it□ □a□e a□so □een add□essed in t□e □ost□□ad□ate □ip□oma in □□□e□ □ec□□it□ p□o□□amme doc□ment□

National College of Ireland

MSc in Cyber Security
New Programme Validation Response Document

Conditions

Recommendations

Postgraduate Diploma in Cyber Security
New Programme Validation Response Document

The differences that exist between the two documents created for the MSc in Cyber Security and Postgraduate Diploma in Cyber Security programmes are listed below:

- The programme proposed structure is different. Postgraduate Diploma is a 60 credits course while the Masters course is 90 credits. The Masters course has 2 extra modules: Research Methods (5 credit) and Internship (25 credits).
- The Minimum Intended Programme Learning Outcomes (MIPLO) for the two programmes are different. PG diploma has 7 MIPLO lsited below.
    - MIPLO1: Demonstrate an awareness and critical understanding of security concepts, technologies and tools that support secure application development, application and service vulnerability detection and patching, data and logs retrieval and analysis
    - MIPLO2: Critically assess and appraise the scientific work in a number of cutting-edge Cyber Security topics
    - MIPLO3: Communicate to a range of audiences in both written and verbal media about

the emerging theories and technologies in an articulate and convincing fashion

- MIPLO□: □tilise practical skills, technologies and tools that support secure programming, application and service vulnerability detection and patching, cryptanalysis, security incidents detection and log file analysis
- MIPLO5: Integrate technologies and security concepts to solve a challenging Cyber Security problem and to successfully plan, develop and test a security product within a given context (e.g. cloud computing or forensics).
- MIPLO6: □nalyse, identify and document measures to address vulnerabilities, risks, weaknesses, and other safety aspects relevant to computing systems within a given context (e.g. Cloud computing, or forensics)
- MIPLO7: Independently ac□uire and assess knowledge in new and emerging technologies from the cybersecurity domain.

- Programme ob□ectives are different for the two programmes.
- The emphasis on developing research skills is reduced in the PG Diploma compared to the Masters course due to the 2 modules (30 credits in total), research related that exist only in the Masters programme.

□ll the module related changes recommended and implemented for the MSc in Cyber Security have also been addressed in the Postgraduate Diploma in Cyber Security programme document.

Panel Member Confirmation

To QQI Validation Unit

This is to confirm that I have reviewed the amended documentation from **National College of Ireland** for the programme(s) titled **MSc and PGD in Cybersecurity** submitted in response to a recent panel report to which I contributed.

I can confirm that the amendments made address the conditions set by the panel. Therefore, I recommend this programme to QQI for validation.

Signed

Stephen Sheridan

Date:

July 12th 2016

CERTIFICATE OF VALIDATION

Provider name	National College of Ireland
Date of validation	20 July 2016

	First Intake	**Last Intake**
Enrolment interval	September 2016	September 2020

	Code	**Title**	**Award**
Principal programme		MSc in Cybersecurity	Master of Science
Embedded programme		Postgraduate Diploma in Science in Cybersecurity	Postgraduate Diploma in Science
Embedded programme			

	Name	**Maximum number of learners**	**Minimum number of learners**
Approved centre	National College of Ireland	As per the validated programmes	As per the validated programmes

Target learner groups	As per the validated programmes
Approved countries for provision	Ireland
The teaching and learning modalities	As per the validated programmes
Brief synopsis of the programme (e.g. who it is for, what is it for, what is involved for learners, what it leads to.)	As per the validated programmes
Specifications for teaching staff	As per the validated programmes
Specifications for the ratio of learners to teaching-staff	As per the validated programmes

Programmes being replaced		
Code	**Title**	**Comment**
		N/A

Conditions of validation

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

a) 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,
b) 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,
c) continue to comply with section 65 of the 2012 Act in respect of arrangements for the protection of enrolled learners, if applicable, and
d) 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.

Conditions from HET Core Validation Policy and Criteria 2010, Revised 2013

The provider of the programme shall (for each programme):

1. Maintain the status of the programme(s) recognition;
2. Establish, having regard to existing quality assurance procedures, procedures for quality assurance for the purpose of further improving and maintaining the quality of education and training which is provided, organised or procured by that provider as part of the programme(s) concerned, and agree those procedures with QQI;
3. Operate quality assurance procedures agreed with QQI;
4. Implement procedures for the assessment of learners which are consistent with Assessment and Standards, Revised 2013;
5. Implement the procedures described in the document Policies, Actions and Procedures for Access, Transfer and Progression for Learners;
6. Implement any special conditions of validation attached to the relevant awards standards.

Other conditions from HET Core Validation Policy and Criteria 2010, Revised 2013

7. Notify QQI of any change in circumstances affecting the provider which could affect or be perceived to affect the provision of the programme(s). This includes significant changes in corporate or academic governance, ownership, legal status, profile of teaching staff, profile of learners, numbers enrolled, facilities, or resources;
8. Maintain learner data records (personal identification, progression, module marks, stage classification etc.) in order to assist QQI in the performance of its functions;
9. Provide the information required by QQI's award making and monitoring functions, including information in respect of completion rates;
10. Implement the programme in accordance with the **approved programme schedule(s)** (appended) and current assessment strategies;
11. Subject to Section 4.6.1 of *HET Core Validation Policy and Criteria 2010*, Revised 2013, obtain QQI's approval prior to substantially amending the programme's minimum intended learning outcomes, save in the case of incremental enhancements arising from the implementation of findings of the provider's agreed quality assurance procedures;
12. Notify QQI of any information concerning the programme(s), or circumstances that may reasonably be expected to give QQI cause to consider reviewing the programme. Explicitly this includes where another awarding body withdraws or seeks to withdraw validation from the programme(s) and /or any alterations to accreditations (additions or withdrawals) by a professional or regulatory body;
13. Implement the programme(s) as agreed with the resources indicated;
14. Adhere to, and implement the Provider Lifecycle of Engagements.

Approved Programme Schedule(s)

Name of Provider	National College of Ireland
Programme Title (i.e. named award)	MSc in Cyber Security
Award Title (QQI named award)	MSc in Cyber Security
Stage Exit Award Title	Postgraduate Diploma in Science in Cyber Security
Modes of Delivery (FT/PT/ACCS/BLENDED/OC etc.)	FT, Blended, Block, ACCS

Award Class	Award NQF Level	Award EQF Level	Stage	Stage NQF Level	Stage EQF Level	Stage Credit (ECTS)	Date Effective	ISCED Subject Code
Major	9		Award	9		90	September 2016	481

Ref	Module Title	Semester	Module		ECTS Credit Number	Total Student Effort			Allocation of Marks			
			Status (M/E)	NQF Level		Total Hours	Contact Hours	Independent Learning	CA %	Project %	Exam %	Total %
	Security Fundamentals	1	M	9	10	250	48	202	40	0	60	100
	Secure Programming for Web	1	M	9	10	250	60	190	60	40	0	100
	IT Law and Ethics	1	M	9	5	125	24	101	40	0	60	100
	Network Security and Penetration Testing	1	M	9	5	125	24	101	40	0	60	100
	Research in Computing	2	M	9	5	125	24	101	20	80	0	100
	Secure Programming for Application Development	2	M	9	5	125	36	89	60	40	0	100
	Cryptography	2	M	9	5	125	24	101	40	0	60	100
	Malware Analysis	2	GE1A, GE2A	9	5	125	24	101	60	40	0	100
	Domain Context	2	GE1B, GE2B	9	5	125	24	101	100	0	0	100
	Incident Response and Analytics	2	GE1	9	5	125	24	101	40	0	60	100
	Forensics and eDiscovery	2	GE1	9	5	125	24	101	40	0	60	100
	Cloud Security	2	GE2	9	10	250	48	202	0	40	60	100
	Research Methods	3	M	9	5	125	24	101	60	40	0	100
	Internship	3	M	9	25	600	10	490	0	100	0	100

Special Regulations:
Note 1: A student must pass Research in Computing and not repeat more than 10 ECTS credits to be eligible to register for the Internship
Note 2: Learners must complete and pass Internship.

Note 3: **Students must choose ONE Group Elective**
Group Elective 1 – Forensics (Modules: Incident Response and Analytics, Forensics and eDiscovery, Cryptography ,and Malware Analysis or Domain Context
Group Elective 2 – Cloud Security (Modules: Cloud Security, Cryptography and Malware Analysis or Domain Context

Note 4: Students from each group elective must to select a 5 credits module from a set of elective modules such as: Malware Analysis or Domain Context.
Note 5: Domain Context module may have a number of instances within the same semester it runs. For example, a different module instance for each specialisation.

Name of Provider	National College of Ireland
Programme Title (i.e. named award)	Postgraduate Diploma in Cyber Security
Award Title (QQI named award)	Postgraduate Diploma in Cyber Security
Stage Exit Award Title	Postgraduate Diploma in Science in Cyber Security
Modes of Delivery (FT/PT/ACCS/BLENDED/OC etc.)	FT, Blended, Block, ACCS

Award Class	Award NQF Level	Award EQF Level	Stage	Stage NQF Level	Stage EQF Level	Stage Credit (ECTS)	Date Effective	ISCED Subject Code
Major	9		Award	9		90	September 2016	481

Ref	Module Title	Semester	Module		ECTS Credit Number	Total Student Effort			Allocation of Marks			
			Status (M/E)	NQF Level		Total Hours	Contact Hours	Independent Learning	CA %	Project %	Exam %	Total %
	Security Fundamentals	1	M	9	10	250	48	202	40	0	60	100
	Secure Programming for Web	1	M	9	10	250	60	190	60	40	0	100
	IT Law and Ethics	1	M	9	5	125	24	101	40	0	60	100
	Network Security and Penetration Testing	1	M	9	5	125	24	101	40	0	60	100
	Research in Computing	2	M	9	5	125	24	101	20	80	0	100
	Secure Programming for Application Development	2	M	9	5	125	36	89	60	40	0	100
	Cryptography	2	M	9	5	125	24	101	40	0	60	100
	Malware Analysis	2	GE1A, GE2A	9	5	125	24	101	60	40	0	100
	Domain Context	2	GE1B, GE2B	9	5	125	24	101	100	0	0	100
	Incident Response and Analytics	2	GE1	9	5	125	24	101	40	0	60	100
	Forensics and eDiscovery	2	GE1	9	5	125	24	101	40	0	60	100
	Cloud Security	2	GE2	9	10	250	48	202	0	40	60	100

Special Regulations:
Note 1: **Students must choose ONE Group Elective**
Group Elective 1 – Forensics (Modules: Incident Response and Analytics, Forensics and eDiscovery, Cryptography ,and Malware Analysis or Domain Context
Group Elective 2 – Cloud Security (Modules: Cloud Security, Cryptography and Malware Analysis or Domain Context

Note 2: Students from each group elective must to select a 5 credits module from a set of elective modules such as: Malware Analysis or Domain Context.
Note 3: Domain Context module may have a number of instances within the same semester it runs. For example, a different module instance for each specialisation.