CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Report of Validation Panel

Date of Meeting: **June 24th, 2020**

Award Type: **Master of Science**

Programme Title: **Master of Science in Cybersecurity Management**

Award Class: **Major**

NFQ Level: **9**

Intakes Commencing: **Sept 2020**

ECTS/ACCS Credits: **90**

CIT Award Standard: **Computing**

Embedded Exit Award: **Yes**

Award Type: **PGD**

Programme Title: **Postgraduate Diploma in Cybersecurity Management**

Award Class: **Major**

NFQ Level: **9**

Intakes Commencing: **Sept 2020**

ECTS/ACCS Credits: **60**

CIT Award Standard: **Computing**

Embedded Exit Award: **No**

PANEL CHAIR

Name, Function, Institution/Organisation
Richard Butler, Dept. of Computing and Networking, IT Carlow

PANEL MEMBERS

Name, Function, Institution/Organisation
Dr Sean Duignan, Head of Dept. of Computer Science & Applied Physics, GMIT
Pat Larkin, CEO Ward Solutions
Jerry Teahan, Global Director Digital Cybersecurity, Johnson Controls
Kim Mulcahy, Module Moderator, Office of Registrar & Vice-President for Academic Affairs, CIT

CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

PROPOSING TEAM MEMBERS

Name, Function, Institution/Organisation
Dr. Saqib Rasool Chaudhry, lecturer, Dept of Computer Science, CIT
Noreen Gubbins, lecturer, Dept of Computer Science, CIT
Dr. Sean McSweeney, Programme Coordinator, Dept of Computer Science, CIT
Triona McSweeney, lecturer, Dept of Computer Science, CIT
AnnMarie O'Donoghue, lecturer, Dept of Organisation and Professional Development, CIT
Dr. Donna O'Shea, Head of Dept of Computer Science, CIT
Vincent Ryan, Senior Lecturer, Dept of Computer Science, CIT
Dr. Dylan Smyth, lecturer, Dept of Computer Science, CIT

1.2.1 PANEL DECLARATIONS ON GDPR AND CONFLICT OF INTEREST

a) The chair and members of the New Programme Validation Panel confirm that they agree to the publication of their name, relevant professional function(s) and affiliated institution/organisation in connection with the present validation review, as required under the statutory quality assurance obligations of Cork Institute of Technology as a public provider of higher education in Ireland.

b) In submitting this report, the chair and members of the New Programme Validation Panel furthermore confirm that no real or apparent conflict of interest is present which would prevent, or could be seen to prevent, the panel's independent and impartial evaluation of the proposed programme(s) and award(s).

BACKGROUND TO THE PROPOSED PROGRAMME

Cork and Ireland is currently positioning itself as a cybersecurity centre of excellence and is home to some of the leading cybersecurity companies such as AlienVault, Cylance, eSentire, FireEye, Forcepoint, GetVisibility, IBM, VMware, Johnson Controls, Keeper Security, McAfee, McKesson, Nuix, Qualcomm, SmartTech, Solarwinds, Sonicwall, Sophos, TransUnion, Trend Micro, UTRC to name but a few. These companies currently operate across a diverse range of sectors such as banking, IoT, Telcom, engineering and automotive. Across these sectors, cybersecurity threats and attacks are becoming more complex and sophisticated every day with a host of professional attackers seeking to exploit vulnerabilities for political or financial gain. This complex landscape is exacerbated further with technologies such as the Internet of Things (IoT) and industry 4.0 which have increased the threat and attack surface requiring the development of sophisticated security solutions that consider the entire digital ecosystem. In addition, within this landscape there is a global shortage of skilled cybersecurity professions with 45% of companies reporting they lack the skills and people they need to defend themselves in this increasingly complex landscape.

To ensure that Cork and Ireland remain an attractive location for Foreign Direct investment (FDI) and to support the existing ecosystem of cybersecurity companies across Ireland a new MSc in Cybersecurity Management is being proposed which includes an embedded award: Post Graduate Diploma in Cybersecurity Management. This programme aims to address the critical skills shortage in the area of cybersecurity with a specific focus on producing graduates that can work as cybersecurity or Cybersecurity Management managers. This embedded 60 credit PGD programme has been approved under the Human Capital Initiative (HCI) Pillar 1, 2020.

2 Findings of the Panel

*NOTE: In this report, the term "**Requirement**" is used to indicate an action or amendment which in the view of the Panel **must be undertaken** prior to commencement of the programme, as a **condition of validation**.*

*The term "**Recommendation**" indicates an item to which the Institute, academic unit or programme board should give serious consideration. Normally it is expected that recommendations will be implemented as soon as possible. Progress will be monitored and will be discussed in programmatic review.*

Requirements and recommendations should be accompanied by a short summary of the observations and findings giving rise to them.

*Panels may also make **Commendations** on instances of good design or practice which may merit wider dissemination and may record any other findings which they deem important for the QA record.*

The Panel has considered the documentation provided and has discussed the programme with the proposers. Based on this, the Panel has arrived at a number of Findings, Requirements and Recommendations as follows.

2.2.1 1. Programme-Level Findings

1.1 NEED FOR THE PROGRAMME

Validation Criterion: Is there a convincing need for the programme with a viable level of applications?

Overall Finding: Yes.

The need for the proposed programme was very clearly expressed, with significant industry engagement and support.

Commendations: The panel commended the team for their deep engagement with industry with a member survey and three separate industry engagement sessions. The findings and feedback were used in the module and programme design to ensure that it fills the gap in the market for a more rounded skill set for those with future Cybersecurity roles in leadership and management.

1.2 AWARD AND PROGRAMME OUTCOMES

Validation Criterion: Are the level and type of the proposed award appropriate? Do the minimum intended programme outcomes adequately describe the intended graduate profile, and do they align with the relevant award standard(s) (incl. for any embedded exit awards)?

Overall Finding: Yes

Findings: MSc in Cybersecurity Management and the embedded award Post Graduate Diploma in Cybersecurity Management are appropriate in their designation.

Commendations: The Programme team was commended for the well explained mapping of the Programme Outcomes to CIT's Award Standards.

Requirements: None.

Requirements: The Programme Outcome Delivery mapping in Akari was not fully completed in the Panel documentation, three modules were missing. The Panel requires that these three outstanding modules are fully mapped.

1.3 LEARNING EXPERIENCE

Validation Criterion: Is the learning experience of an appropriate level, standard and quality overall?

Overall Finding: Yes.

The proposed Programme Outcomes as presented to the Panel are attached as Appendix 1.

While the programme was designed for blended learning, delivery to the first cohort will be fully online in 2020/21 as a result of COVID-19. This decision was made to give immediate clarity to students despite the lack of concrete government guidelines. Learning will be maintained remotely with labs completed virtually. This will eliminate the need for the Department to consider a reduction of lab sizes. With the use of virtual Labs there will be no requirement for Personal Protective Equipment or cleaning of equipment between sessions as there would be with a physical lab.

Findings, requirements, and recommendations concerning individual modules (if any) are recorded in Section 2 below.

1.4 PROGRAMME STRUCTURE

Validation Criterion: Is the programme structure logical and well designed (including procedures for access, transfer and progression)?

Overall Finding: Yes

The Panel notes that part of the programme structure had already been the subject of external peer evaluation by the HCI for the Post Graduate Diploma award. The Semester Schedules as proposed are in Appendix 2. The schedule shown shows the module swap that was discussed and approved during the panel meeting.

Findings: The MSc in Cybersecurity Management includes an embedded award: Postgraduate Diploma in Cybersecurity Management. This embedded 60 credit PGD programme (which has been approved under the Human Capital Initiative (HCI) Pillar 1, 2020) offers flexibility to students.

The programme structure is well designed to deliver an appropriate learning environment to candidates on the programme. It was noted that there are free choice electives in semesters one and two, meaning there is no need to seek derogation. The panel noted that two 5 credit modules “cyber contingency planning” and “communications & Cybersecurity” will swap slots between semesters one and two. This will improve delivery as the learners will have a greater understanding for the context of the communications module.

Commendations: None

Requirements: None

Recommendations: The Panel recommends that some minor corrections be made to the programme document. The module titles differ between the programme document and Akari. The programme document section 2.1 and 3.0 references CIT’s Strategic Plan 2012-2016 and enrolment figures, which have been amended. Section 3.8 refers to the QQI as the Designated Awarding Body, CIT was established as a Designated Awarding Body in January 2020.

1.5 PROGRAMME MANAGEMENT

Validation Criterion: Are the programme management structures adequate?
Overall Finding: Yes

Findings: The Department and Programme co-ordinator are experienced with online and on campus delivery from other MSc programmes and have the capacity to add to the suite of programmes offered.

Commendations: None.

Requirements: None.

Recommendations: The Panel recommends that an assessment matrix is published for the programme for clarity for students and to ensure there are no clashes.

1.6 RESOURCE REQUIREMENTS

Validation Criterion: Are the resource requirements reasonable?
Overall Finding: Yes

The Panel was assured on behalf of the President and Head of Faculty/College/School that appropriate resources in terms of staffing and facilities will be put in place when the programme is validated.

Findings: The Department has an existing, recently expanded, cloud environment is used to deliver labs in several security modules. Resources dedicated to the proposed programme to support the additional load existing infrastructure will be sufficient for delivery of the additional labs for the proposed programme.

An analysis was completed to identify gaps in staff training or resources. Training will be completed, and resources purchased so they are available to incoming students in September.

Commendations: None

Requirements: None

Recommendations: None

1.7 IMPACT ON THE INSTITUTE

Validation Criterion: Will the impact of the programme on the Institute be positive?
Overall Finding: Yes

Findings: The panel noted that the programme recognised the need for broader skills in the sector and aims to addresses a lack of diversity and gender inequality in the graduate pool.

Commendations: None.

Requirements: None.

Recommendations: None.

2.2.2 2. Module-Level Findings

The Panel notes that 7 modules on the proposed programme are pre-approved modules which may be delivered across several CIT programmes.

The Panel was informed that the new draft modules have been the subject of internal and external scrutiny by the CIT module moderator and external reviewers.

In exercising its brief to consider the overall standard and appropriateness of modules, the Panel wishes to add the following findings, requirements and recommendations.

2.1 ALL MODULES

Requirement: Any revisions to Module Descriptors or Semester Schedules made to address the recommendations and requirements in this validation panel report require sign-off from the CIT Module Moderator and the Registrar's Office prior to approval by the CIT Academic Council.

There are no recommendations or requirements for approved modules on the programme.

2.2. MODULE:

Findings: There was positive discussion of all of the modules in the programme. The switching of modules between semesters one and two in order to complete Cyber contingency planning first which will allow students to have a greater understanding for the context of the Communications & Cybersecurity module was discussed and approved.

There was a little overlap of indicative content between modules, but this was seen as positive as it was in different contexts and will reinforce important topics. The Emerging Cyber Trends module is an opportunity to have guest lecturers do a deep dive into a particular area of expertise.

Commendations: The panel noted the mix and balance of modules between the semesters, which was beneficial to both student workload and efficiency of delivery. A varied blend of assessment types and timings was also noted. The team was praised for taking a novel approach and using National best practice in designing the Work Based Project module.

Requirements: The programme includes a Security Work Based Project. If it is not possible for a student to complete this in the workplace an alternative module needs to be available.

Recommendations: are detailed below for each individual module.

2.2.1 Security Risk & Compliance i.d. 14793, Expert, 10 ECTS

Recommendations: There is no finance, security contingency planning or auditing included in the indicative content. These should be incorporated.

2.2.2 Security Architecture i.d. 14790, Expert, 10 ECTS

Recommendations: Include rights management, protection of data, penetration testing and costing in the design of the final project. Edge, Zero Trust, Zero-knowledge, perimeter management and Chip-to-Cloud are also not covered.

2.2.3 Communications & Cybersecurity i.d. 14891, Expert, 5 ECTS

Recommendations: Include dialogue control and structure of communications around a data breach.

2.2.4 Security Management and Law i.d. 14797, Expert, 10 ECTS

Recommendations: Add EU Data Protection, NIS Directive and See Saw. Examine responsibilities at different levels and roles such as Security Manager and Security Architect.

2.2.5 Security Work Based Project i.d. 14815, Expert, 10 ECTS

The module requires students to be in employment to complete so an alternative for those not in employment was discussed. If the work based project module does not have the flexibility for amendments to allow completion by those not in employment, (e.g. lack of everyday functions in the workplace such as team management and implementation plans) then an alternative of the proposed Group Project module needs to be added as an option.

Requirements: An alternative to the work-based project module will need to be made available to students without employment.

2.2.6 Security Contingency Planning i.d. 14794, Expert, 5 ECTS

Recommendations: Include how to implement threat assessment, threat intelligence and incident response from a management perspective. This will link to the Emerging Cyber Trends module.

2.2.7 Emerging Cyber Trends i.d. 14812, Advanced, 5 ECTS

Recommendations: Amend the description of the project to make it more open in order to give students more scope in their chosen focus area.

2.2.8 Computing Research Project i.d. 12420, Expert, 30 ECTS

Finding: The Computing Research Project is a generic module used in a number of programmes in the Department.

3. Other Findings

None.

4. Conclusion

Based on the above findings, the Panel has arrived at the following Conclusions:

- The Programme meets the required standards for an award in its field of study at Level 9 of the CIT Awards Standards for Computing.

- The Programme meets the criteria for validation of a new programme adopted by the Academic Council of Cork Institute of Technology.

The Panel therefore recommends that the Programme be validated for five academic years, or until the next programmatic review, whichever is soonest, subject to implementation of the Requirements above, and with due regard to the Recommendations made.

3 Implementation of Requirements and Recommendations

*NOTE: This section is **co-completed by the Academic Department and the CIT Registrar's Office**.*

It records the implementation of any panel requirements and the completion of the internal programme and module moderation process. Confirmation of completion by the CIT Registrar's Office is required for both before the programme is submitted to the CIT Academic Council for validation.

1. IMPLEMENTATION OF PANEL REQUIREMENTS

Requirement(s)	**Department Response**
1.4 Recommendations: The Panel recommends that some minor corrections be made to the programme document. The module titles differ between the programme document and Akari. The programme document section 2.1 and 3.0 references CIT's Strategic Plan 2012-2016 and enrolment figures, which have been amended. Section 3.8 refers to the QQI as the Designated Awarding Body, CIT was established as a Designated Awarding Body in January 2020.	The programme board has updated the references to the older iterations of CITs Strategic Plan and enrolment figures in the sections 2.1 and 3.0. Module titles in the programme document are now aligned to those in Akari. Section 3.8 has also been amended in the updated programme document.
1.5 Recommendations: The Panel recommends that an assessment matrix is published for the programme for clarity for students and to ensure there are no clashes.	Once the programme will be validated this action will be taken. The assessment matrix has been shared with the validation panel in the meantime.
2.2 Requirements: The programme includes a Security Work Based Project. If it is not possible for a student to complete this in the workplace an alternative Group Project needs to be available. The current module descriptor may be used for students in employment. The proposed Group Project module may can be used for those not in employment.	The group-based project module has been added to the programme to accommodate this possibility and this change is reflected in Akari. The department has a long history of running modules such as this at undergraduate level and so the operation of this module will not present an unexpected challenge.
2.2.1 Security Risk & Compliance Recommendations: There is no finance, security contingency planning or auditing included in the indicative content. These should be incorporated.	These elements have been incorporated into the indicative content.
2.2.2 Security Architecture Recommendations: Include rights management, protection of data, penetration testing and costing in the design of the final project. Edge, Zero Trust, Zero-knowledge, perimeter management and Chip-to-Cloud are also not covered.	These elements have been incorporated into the indicative content.

2.2.3 Communications & Cybersecurity Recommendations: Include dialogue control and structure of communications around a data breach.	These elements have been incorporated into the indicative content.
2.2.4 Security Management and Law Recommendations: Add EU Data Protection, NIS Directive and See Saw. Examine responsibilities at different levels and roles such as Security Manager and Security Architect.	These elements have been incorporated into the indicative content.
2.2.5 The module requires students to be in employment to complete so an alternative for those not in employment was discussed. If the work based project module does not have the flexibility for amendments to allow completion by those not in employment, (e.g. lack of everyday functions in the workplace such as team management and implementation plans) then an alternative of the proposed Group Project module needs to be added as an option. Requirements: An alternative to the work-based project module will need to be made available to students without employment.	An alternative group project module has been made available to provide for this contingency. The programme has been modified to facilitate this as a separate elective. Group Project module ID 14823.
2.2.6 Security Contingency Planning Recommendations: Include how to implement threat assessment, threat intelligence and incident response from a management perspective. This will link to the Emerging Cyber Trends module.	These elements have been incorporated into the indicative content.
2.2.7 Emerging Cyber Trends Recommendations: Amend the description of the project to make it more open in order to give students more scope in their chosen focus area.	The project descriptor has been amended to facilitate a greater scope.

2. SIGN-OFF ON FINAL PROGRAMME SPECIFICATION (INCLUDING MODULES)

[This section to be completed by the CIT Registrar's Office]

The CIT Registrar's Office confirms that:

- The Programme and Module Moderation Process for this proposed programme is complete; and
- The final Programme Specification and associated Module Descriptors are deemed ready to be submitted to Academic Council for approval.

Signed: ___ **Date: ___**

CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

APPENDIX 1 (A) – PROPOSED MSC PROGRAMME OUTCOMES MAPPED TO CIT AWARD STANDARD – COMPUTING LEVEL 9

		Mapping of CIT Programme Outcomes to:	
		CIT Award Standard – Computing Level 9	
Generic Standard Level 9	Computing Standard Level 9	MSc in Cybersecurity Management Programme Outcomes	Supporting Statement
Knowledge-Breadth			
The graduate should be able to demonstrate: *A systematic understanding of knowledge at, or informed by, the forefront of a field of learning*	The learner will have expert knowledge of one or more current state-of-the-art specialist computing areas and will be able to demonstrate knowledge of relevant research methodologies	A mastery of the theoretical knowledge and applied skills necessary determine how Cybersecurity governance, risk and compliance enable the alignment of security architecture, engineering and operations to meet business goals. The student will also be able to master other specialist areas of Cybersecurity by taking electives that match their interests.	The learner will develop the ability to discriminate between different cybersecurity threats and their impact on business operational elements, appraise the application of cybersecurity controls and technologies used by an organisation to detect and respond to a successful attack among other skills in *"Security Risk and Compliance"* and *"Security Architecture"* respectively. The learner will develop specific specialist knowledge such as the how to hack a website with the purpose of identifying its specific vulnerabilities and hardening the website against attacks and appraising business level and corporate level strategies in relation to competitive and global environmental changes in *"Scripting for Cybersecurity"* and *"Strategic Thinking"* respectively. This knowledge will develop their capacity to become an effective cybersecurity manager.
Knowledge-Kind			
The graduate should be able to demonstrate: *A critical awareness of current problems and/or new insights generally informed by the forefront of a field of learning*	The learner will be able to: 1. demonstrate an awareness and critical understanding of developments in a number of specialist areas in computing. 2. discuss current challenges and research activities in at least one of these areas. 3. apply accepted methodologies for tackling research problems.	A critical understanding and appraisal of a number of specialist areas in cybersecurity; discuss current challenges and research activities in these areas and apply accepted methodologies for tackling research problems.	Through *"Emerging Cyber Trends"* the learner will critique emerging and current enterprise cybersecurity trends with the aim of building a cybersecurity program developing a deep understanding of the current security landscape. The learner will also develop the necessary understanding to analyse and model the mathematical foundations to modern cryptographic techniques and apply this understanding to critically evaluate modern symmetric and asymmetric cryptographic techniques and discuss the current challenges and emerging work in cryptography and its implications for enterprise systems at differing scales in *"Applied Cryptography"*. The learner will apply statistical algorithms to anomaly detection for a specific application domain and thus develop a methodology to approach online anomaly detection over big-data streams in *"Fraud and Anomaly Detection"*. This knowledge will be further developed in *"Computing Research Project"* where the learner will select and implement appropriate research methods and techniques with the aim of identifying a research question in cybersecurity.
Know-How & Skill-range			
The graduate should be able to demonstrate: *A range of standard and specialised research or equivalent tools and techniques*	The learner will be able to: 1. select and apply standard and customised research tools and techniques of enquiry forming a solid foundation for pursuing further research.	Evaluate and apply research tools and techniques of inquiry; investigate current challenges in Cybersecurity practice and research; formulate appropriate strategies from emerging theories; communicate to a range of audiences in both written and	The learner will develop the capacity to apply a standardised technique of enquiry to a wide range of activities and operational contexts. The learner will develop the ability to perform a threat assessment and modelling with the aim of optimising network security measures and critically assess the security of a cloud based virtualised infrastructure with the aim of protecting data, application and services of cloud computing resources in

of enquiry	2. critically evaluate design and implementation issues in particular application areas depending on the research undertaken. 3. communicate to a range of audiences in both written and verbal media about new and emerging theories and technologies in an articulate and convincing fashion. 4. integrate advanced theoretical knowledge and solve complex problems in new, ill-defined or unfamiliar domains and/or domains at the forefront of learning. 5. critically evaluate and synthesise the academic research and professional literature base. 6. exhibit his/her research capabilities in a number of cutting-edge computing topics, demonstrating an understanding of the changing knowledge base in these topics. 7. independently acquire and assess knowledge in novel and emerging technologies	verbal media cutting edge work in the field of Cybersecurity.	*"Security Architecture"*. However, the learner will also develop the skill to synthesise the ethical, business and social aspects of communicating technology-centred concepts for a non-technical audience while demonstrating understanding of cyber-security concepts and defend both their evaluation and recommendations of strategic management issues in *"Communications and Cybersecurity"*. Specific exercise scenarios will occur in the programme that will require the learner to use advanced knowledge to solve problems in ill-defined domains such as critiquing a disaster recovery plan for efficacy and adherence to regulations and legal requirements which will require the learner to evaluate current professional literature in *"Contingency Planning"*. The learner will apply appropriate written and oral communication skills and synthesise the research work in the form of presentations, abstracts, executive summaries, technical papers and a dissertation in *"Computing Research Project"*.
Know-How & Skill-Selectivity			
The graduate should be able to demonstrate: *Selection from complex and advanced skills across a field of learning; development of new skills to a high level, including novel and emerging techniques*	The learner will be able to: 1. Independently acquire and assess knowledge in novel and emerging technologies. 2. integrate knowledge of various technologies and computing principles to successfully plan and develop a computer-based project. 3. apply existing and develop new research skills to plan and implement a research project to solve a challenging computing problem. 4. formulate judgements and synthesise conclusions following the completion of a systematic piece of research. *5.* select and apply standard and customised research tools and techniques of enquiry forming a solid foundation for pursuing further research.	Develop the necessary skills to plan and implement a work-based project incorporating novel and emerging practices and technologies to develop a solution to a complex problem in Cybersecurity.	The learner will develop the capability in *"Security Work Based Project"* to independently acquire and assess knowledge by autonomously managing learning in their work-based project without the need for formal instruction demonstrating their ability to take ownership of their learning and performance in the workplace. The learner will develop a project scope and definition aligned to the programme of study which integrates the knowledge of various technologies and techniques in cybersecurity. The learner will plan and organise activities related to the project within a limited timeframe and interpret, evaluate, document and present project findings and effectively communicate with peers in the organisation who work in different roles and across the organisation with the aim of achieving the project objectives. The learner will develop a contribution to cybersecurity knowledge in *"Computing Research Project" and* prepare a thesis that details and evaluates the work undertaken and justifies the conclusions reached.
Competence-Context			
The graduate should be able to demonstrate:	The learner will be able to:	Analyse and document measures to address risks and weaknesses in Cybersecurity	The learner will be able to operate in a wide and unpredictable range of levels and contexts after completing this programme due to the wide

Action in a wide and often unpredictable variety of professional levels and ill-defined contexts	1. analyse and document measures to address risks or safety aspects relevant to computing systems within a given context. 2. evaluate existing and develop new best practices in a range of real-world contexts. 3. develop guidelines regarding professional, ethical and legal practices in the exploitation of computer technology. 4. design and implement a computing solution that requires significant preliminary research for novel and unfamiliar situations. 5. evaluate existing and develop new diagnostic models in a range of contexts. 6. identify potential projects and research opportunities. 7. conduct appropriate research and undertake the design and development of computing solutions. *8.* demonstrate an appreciation of the professional standards relevant to the computing discipline.	policy and procedures; develop guidelines regarding professional and ethical practices in Cybersecurity; design and implement management frameworks and practices with the aim of improving an organisation's security posture and enhance resilience's against cyberattacks.	variety of content delivered in this programme, from highly technical in the operations of specific cybersecurity activities, such as web application penetration testing in *"Scripting for Cybersecurity"* to the highly strategic such as critiquing a disaster recovery plan for efficacy and adherence to regulations and legal requirements in *"Contingency Planning"*. Other modular learning outcomes in this programme which include activities such as developing a cybersecurity risk management plan to analysing cybersecurity compliance standards and frameworks in *"Security Risk and Compliance"* to appraising the application of cybersecurity controls and technologies used by an organisation to prevent an attack in *"Security Architecture"* or critically evaluating security models and frameworks in their ability to serve as a roadmap to organise cybersecurity management activities in an organisation in *"Security Management and Law"* ensure a well-rounded graduate highly capable of both role and context switching as necessary in their further career. In *"Computing Research Project"* the learner will plan and implement self-directed learning to further knowledge and understanding of an unfamiliar and/or ill-defined problem in cybersecurity. The learner will undertake a significant body of work in *"Computing Research Project"* which will require them to design and implement a solution derived from existing literature to a cybersecurity challenge.
Competence-role			
The graduate should be able to demonstrate: *Taking significant responsibility for the work of individuals and groups; lead and initiate activity*	The learner will be able to: 1. initiate, lead and manage projects of significant complexity involving multi-disciplinary teams. 2. work as a member of an IT strategic planning team. 3. participate in peer collaboration and evaluation exercises	Develop the competence required to lead and manage projects in Cybersecurity involving multidisciplinary teams in medium/large organizations; communicate the complexities of Cybersecurity technical project elements to strategic leadership teams in an organisation; Evaluate Cybersecurity risks with the aim of preparing an organisation against likely attacks.	The learner will develop the necessary competence to initiate, lead and manage the human aspect of projects of significant scale and complexity through developing knowledge on how to apply the strategic issues involved in the management of human resources to an international context, critically evaluate different international perspectives on human resource management, analyse international human resource management strategies for managing people in various locations and be able to appraise the challenges of corporate social responsibility and its relationship to international human resources management in *"People Management Strategies"*. The learner will develop the necessary competence to manage the governance, risk and compliance aspects of such projects through developing the capacity to review and adapt policy and standards with the aim of developing a security program and evaluate security management practices in managing an organisations information assets in areas such as privacy, confidentiality, integrity and accountability in *"Security Risk and Compliance"* and *"Security Architecture"* respectively. In *"Computing Research Project"* the learner will work closely with their project supervisor and through this relationship develop an understanding of the scientific peer collaboration and evaluation process.

Competence-Learning to Learn			
The graduate should be able to demonstrate: *Learning to self-evaluate and take responsibility for continuing academic/professional development*	The learner will be able to: 1. reflect on the strengths, weaknesses and potential for future development of his/her own work. 2. demonstrate an understanding of the importance of continuing personal development in the computing discipline and the mechanisms and resources available to support that learning.	Develop the knowledge to formulate an appropriate continuing professional development plan based on personal goals. Acquire the knowledge and skills to independently learn and understand Cybersecurity trends to direct new self-directed learning and manage the learning pathway of a cybersecurity team.	This programme develops in the learner significant capacity to self-evaluate and execute a continued professional development in several differing ways. The learner will develop the capacity to maintain a clear CPD plan through *"Security Work Based Project"* by managing learning without the need for formal instruction demonstrating their ability to take ownership of their learning and performance in the workplace. The learner will form the understanding of the ever changing nature of cybersecurity and develop the capacity to maintain their knowledge of this landscape through critiquing emerging and current enterprise cybersecurity trends with the aim of building a cybersecurity program in *"Emerging Cyber Trends"* and discriminating between different cybersecurity threats and their impact on business operational elements in *"Security Risk and Compliance"*. The learner will also develop the capacity to critically interpret, analyse and evaluate key aspects of the learning process, from the learners own personal perspective in *"Strategic Thinking"*. The learner will be required to implement self-directed learning to develop the necessary understanding to undertake their major project in *"Computing Research Project"*, as this work will span a number of months the value of CPD to tackle longer term projects will be imparted on the learner.
Competence-Insight			
The graduate should be able to demonstrate: *Scrutinising and reflecting on social norms and relationships and acting to change them*	The learner will be able to: 1. critically comment on the technical and social implications of his/her own work and the work of others. 2. demonstrate a critical appreciation of the design issues in developing a computing system, taking into account the environment in which it is used. 3. evaluate the way that computing technology is currently affecting society and reflect on its potential future effect. 4. maintain integrity and independence in professional judgement.	Expert knowledge in assessing the risk of emerging threats in Cybersecurity and applying governance and management countermeasures in compliance with legal and industry standards to mitigate these threats.	The ability to scrutinise and reflect on social norms and relationships and the capacity to act on them to effect change will be developed in the learner though many of the actives undertaken in this programme. On the highly technical side of cybersecurity the learner will learn how to appraise the security of deployed cryptographic systems and evaluate modern cryptographic techniques, such as Digital Signatures and Hashing and their implication for societal concerns such as digital privacy and public security in *"Applied Cryptography"*. The learner will develop a sophisticated understanding of his/her ethical responsibilities as a cybersecurity manager with access to and responsibility for a significant quantity of sensitive information through appraising the challenges of corporate social responsibility and evaluating the trade-offs in differing technical and management approaches in cybersecurity in *"Security Management and Law"*. In preparing a thesis that details and evaluates the work undertaken and justifies the conclusions reached in *"Computing Research Project"* the learner will develop the ability to critically comment on the implications of their work and how to evaluate it to other contemporary work.

CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

APPENDIX 1 (B) – PROPOSED PGD PROGRAMME OUTCOMES MAPPED TO CIT AWARD STANDARD – COMPUTING LEVEL 9

		Mapping of CIT Programme Outcomes to:	
		CIT Award Standard – Computing Level 9	
Generic Standard Level 9	Computing Standard Level 9	PGD in Cybersecurity Management Programme Outcomes	Supporting Statement
Knowledge-Breadth			
The graduate should be able to demonstrate: *A systematic understanding of knowledge at, or informed by, the forefront of a field of learning*	The learner will have expert knowledge of one or more current state-of-the-art specialist computing areas and will be able to demonstrate knowledge of relevant research methodologies	A mastery of the theoretical knowledge and applied skills necessary determine how Cybersecurity governance, risk and compliance enable the alignment of security architecture, engineering and operations to meet business goals. The student will also be able to master other specialist areas of Cybersecurity by taking electives that match their interests.	The learner will develop the ability to discriminate between different cybersecurity threats and their impact on business operational elements, appraise the application of cybersecurity controls and technologies used by an organisation to detect and respond to a successful attack among other skills in *"Security Risk and Compliance"* and *"Security Architecture"* respectively. The learner will develop specific specialist knowledge such as the how to hack a website with the purpose of identifying its specific vulnerabilities and hardening the website against attacks and appraising business level and corporate level strategies in relation to competitive and global environmental changes in *"Scripting for Cybersecurity"* and *"Strategic Thinking"* respectively. This knowledge will develop their capacity to become an effective cybersecurity manager.
Knowledge-Kind			
The graduate should be able to demonstrate: *A critical awareness of current problems and/or new insights generally informed by the forefront of a field of learning*	The learner will be able to: 4. demonstrate an awareness and critical understanding of developments in a number of specialist areas in computing. 5. discuss current challenges and research activities in at least one of these areas. 6. apply accepted methodologies for tackling research problems.	A critical understanding and appraisal of a number of specialist areas in cybersecurity; discuss current challenges and research activities in these areas and apply accepted methodologies for tackling research problems.	Through *"Emerging Cyber Trends"* the learner will critique emerging and current enterprise cybersecurity trends with the aim of building a cybersecurity program developing a deep understanding of the current security landscape. The learner will also develop the necessary understanding to analyse and model the mathematical foundations to modern cryptographic techniques and apply this understanding to critically evaluate modern symmetric and asymmetric cryptographic techniques and discuss the current challenges and emerging work in cryptography and its implications for enterprise systems at differing scales in *"Applied Cryptography"*. The learner will apply statistical algorithms to anomaly detection for a specific application domain and thus develop a methodology to approach online anomaly detection over big-data streams in *"Fraud and Anomaly Detection"*.
Know-How & Skill-range			
The graduate should be able to demonstrate: *A range of standard and specialised research or equivalent tools and techniques of enquiry*	The learner will be able to: 8. select and apply standard and customised research tools and techniques of enquiry forming a solid foundation for pursuing further research. 9. critically evaluate design and implementation issues in particular	Evaluate and apply research tools and techniques of inquiry; investigate current challenges in Cybersecurity practice and research; formulate appropriate strategies from emerging theories; communicate to a range of audiences in both written and verbal media cutting edge work in the field of Cybersecurity.	The learner will develop the capacity to apply a standardised technique of enquiry to a wide range of activities and operational contexts. The learner will develop the ability to perform a threat assessment and modelling with the aim of optimising network security measures and critically assess the security of a cloud based virtualised infrastructure with the aim of protecting data, application and services of cloud computing resources in *"Security Architecture"*. However, the learner will also develop the skill to synthesise the ethical, business and social aspects of communicating

	application areas depending on the research undertaken. 10. communicate to a range of audiences in both written and verbal media about new and emerging theories and technologies in an articulate and convincing fashion. 11. integrate advanced theoretical knowledge and solve complex problems in new, ill-defined or unfamiliar domains and/or domains at the forefront of learning. 12. critically evaluate and synthesise the academic research and professional literature base. 13. exhibit his/her research capabilities in a number of cutting-edge computing topics, demonstrating an understanding of the changing knowledge base in these topics. 14. independently acquire and assess knowledge in novel and emerging technologies		technology-centred concepts for a non-technical audience while demonstrating understanding of cyber-security concepts and defend both their evaluation and recommendations of strategic management issues in *"Communications and Cybersecurity"*. Specific exercise scenarios will occur in the programme that will require the learner to use advanced knowledge to solve problems in ill-defined domains such as critiquing a disaster recovery plan for efficacy and adherence to regulations and legal requirements which will require the learner to evaluate current professional literature in *"Contingency Planning"*.
Know-How & Skill-Selectivity			
The graduate should be able to demonstrate: *Selection from complex and advanced skills across a field of learning; development of new skills to a high level, including novel and emerging techniques*	The learner will be able to: 6. Independently acquire and assess knowledge in novel and emerging technologies. 7. integrate knowledge of various technologies and computing principles to successfully plan and develop a computer-based project. 8. apply existing and develop new research skills to plan and implement a research project to solve a challenging computing problem. 9. formulate judgements and synthesise conclusions following the completion of a systematic piece of research. *10.* select and apply standard and customised research tools and techniques of enquiry forming a solid foundation for pursuing further research.	Develop the necessary skills to plan and implement a work-based project incorporating novel and emerging practices and technologies to develop a solution to a complex problem in Cybersecurity.	The learner will develop the capability in *"Security Work Based Project"* to independently acquire and assess knowledge by autonomously managing learning in their work-based project without the need for formal instruction demonstrating their ability to take ownership of their learning and performance in the workplace. The learner will develop a project scope and definition aligned to the programme of study which integrates the knowledge of various technologies and techniques in cybersecurity. The learner will plan and organise activities related to the project within a limited timeframe and interpret, evaluate, document and present project findings and effectively communicate with peers in the organisation who work in different roles and across the organisation with the aim of achieving the project objectives.
Competence-Context			
The graduate should be able to demonstrate: ***Action in a wide and often***	The learner will be able to: 9. analyse and document measures to address risks or safety aspects relevant to computing	Analyse and document measures to address risks and weaknesses in Cybersecurity policy and procedures; develop guidelines regarding professional and ethical practices	The learner will be able to operate in a wide and unpredictable range of levels and contexts after completing this programme due to the wide variety of content delivered in this programme, from highly technical in the operations of specific cybersecurity activities, such as web application

unpredictable variety of professional levels and ill-defined contexts	systems within a given context. 10. evaluate existing and develop new best practices in a range of real-world contexts. 11. develop guidelines regarding professional, ethical and legal practices in the exploitation of computer technology. 12. design and implement a computing solution that requires significant preliminary research for novel and unfamiliar situations. 13. evaluate existing and develop new diagnostic models in a range of contexts. 14. identify potential projects and research opportunities. 15. conduct appropriate research and undertake the design and development of computing solutions. *16.* demonstrate an appreciation of the professional standards relevant to the computing discipline.	in Cybersecurity; design and implement management frameworks and practices with the aim of improving an organisation's security posture and enhance resilience's against cyberattacks.	penetration testing in *"Scripting for Cybersecurity"* to the highly strategic such as critiquing a disaster recovery plan for efficacy and adherence to regulations and legal requirements in *"Contingency Planning"*. Other modular learning outcomes in this programme which include activities such as developing a cybersecurity risk management plan to analysing cybersecurity compliance standards and frameworks in *"Security Risk and Compliance"* to appraising the application of cybersecurity controls and technologies used by an organisation to prevent an attack in *"Security Architecture"* or critically evaluating security models and frameworks in their ability to serve as a roadmap to organise cybersecurity management activities in an organisation in *"Security Management and Law"* ensure a well-rounded graduate highly capable of both role and context switching as necessary in their further career.
Competence-role			
The graduate should be able to demonstrate: *Taking significant responsibility for the work of individuals and groups; lead and initiate activity*	The learner will be able to: 4. initiate, lead and manage projects of significant complexity involving multi-disciplinary teams. 5. work as a member of an IT strategic planning team. 6. participate in peer collaboration and evaluation exercises	Develop the competence required to lead and manage projects in Cybersecurity involving multidisciplinary teams in medium/large organizations; communicate the complexities of Cybersecurity technical project elements to strategic leadership teams in an organisation; Evaluate Cybersecurity risks with the aim of preparing an organisation against likely attacks.	The learner will develop the necessary competence to initiate, lead and manage the human aspect of projects of significant scale and complexity through developing knowledge on how to apply the strategic issues involved in the management of human resources to an international context, critically evaluate different international perspectives on human resource management, analyse international human resource management strategies for managing people in various locations and be able to appraise the challenges of corporate social responsibility and its relationship to international human resources management in *"People Management Strategies"*. The learner will develop the necessary competence to manage the governance, risk and compliance aspects of such projects through developing the capacity to review and adapt policy and standards with the aim of developing a security program and evaluate security management practices in managing an organisations information assets in areas such as privacy, confidentiality, integrity and accountability in *"Security Risk and Compliance"* and *"Security Architecture"* respectively.
Competence-Learning to Learn			
The graduate should be able to demonstrate: *Learning to self-evaluate and take responsibility for*	The learner will be able to: 3. reflect on the strengths, weaknesses and potential for future development of his/her own work.	Develop the knowledge to formulate an appropriate continuing professional development plan based on personal goals. Acquire the knowledge and skills to independently learn and understand	This programme develops in the learner significant capacity to self-evaluate and execute a continued professional development in several differing ways. The learner will develop the capacity to maintain a clear CPD plan through *"Security Work Based Project"* by managing learning without the need for formal instruction

continuing academic/professional development	4. demonstrate an understanding of the importance of continuing personal development in the computing discipline and the mechanisms and resources available to support that learning.	Cybersecurity trends to direct new self-directed learning and manage the learning pathway of a cybersecurity team.	demonstrating their ability to take ownership of their learning and performance in the workplace. The learner will form the understanding of the ever changing nature of cybersecurity and develop the capacity to maintain their knowledge of this landscape through critiquing emerging and current enterprise cybersecurity trends with the aim of building a cybersecurity program in *"Emerging Cyber Trends"* and discriminating between different cybersecurity threats and their impact on business operational elements in *"Security Risk and Compliance"*. The learner will also develop the capacity to critically interpret, analyse and evaluate key aspects of the learning process, from the learners own personal perspective in *"Strategic Thinking"*.
Competence-Insight			
The graduate should be able to demonstrate: *Scrutinising and reflecting on social norms and relationships and acting to change them*	The learner will be able to: 5. critically comment on the technical and social implications of his/her own work and the work of others. 6. demonstrate a critical appreciation of the design issues in developing a computing system, taking into account the environment in which it is used. 7. evaluate the way that computing technology is currently affecting society and reflect on its potential future effect. 8. maintain integrity and independence in professional judgement.	Expert knowledge in assessing the risk of emerging threats in Cybersecurity and applying governance and management countermeasures in compliance with legal and industry standards to mitigate these threats.	The ability to scrutinise and reflect on social norms and relationships and the capacity to act on them to effect change will be developed in the learner though many of the actives undertaken in this programme. On the highly technical side of cybersecurity the learner will learn how to appraise the security of deployed cryptographic systems and evaluate modern cryptographic techniques, such as Digital Signatures and Hashing and their implication for societal concerns such as digital privacy and public security in *"Applied Cryptography"*. The learner will develop a sophisticated understanding of his/her ethical responsibilities as a cybersecurity manager with access to and responsibility for a significant quantity of sensitive information through appraising the challenges of corporate social responsibility and evaluating the trade-offs in differing technical and management approaches in cybersecurity in *"Security Management and Law"*.

CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

APPENDIX 2 – SEMESTER SCHEDULES

Stage 1 / Semester 1

Mandatory								
Mod Code	**Module Title**	**Co-ordinator**	**Level**	**Credits**	**FT Contact Hours**	**PT Contact Hours**	**Course Work**	**Formal Exam**
No Code Yet	Security Risk & Compliance (Draft)	Donna OShea	Expert	10.0	6.00	6.00	100.0	0.0
No Code Yet	Security Architecture (Draft)	Donna OShea	Expert	10.0	6.00	6.00	100.0	0.0
No Code Yet	Security Contingency Planning (Draft)	Donna OShea	Expert	5.0	4.00	4.00	100.0	0.0

Elective								
Mod Code	**Module Title**	**Co-ordinator**	**Level**	**Credits**	**FT Contact Hours**	**PT Contact Hours**	**Course Work**	**Formal Exam**
COMP9053	Scripting for Cybersecurity (Draft)	Donna OShea	Expert	5.0	4.00	4.00	100.0	0.0
MGMT9034	Strategic Thinking (Approved)	Pio Fenton	Expert	5.0	2.00	2.00	100.0	0.0
FREE6001	Free Choice Module (Approved)	PAUL GALLAGHER	N/A	5.0	4.00	0.00	50.0	50.0

Stage 1 / Semester 2

Mandatory								
Mod Code	**Module Title**	**Co-ordinator**	**Level**	**Credits**	**FT Contact Hours**	**PT Contact Hours**	**Course Work**	**Formal Exam**
No Code Yet	Security Management and Law (Draft)	Donna OShea	Expert	10.0	6.00	6.00	100.0	0.0
No Code Yet	Security Work Based Project (Draft)	Donna OShea	Expert	10.0	0.50	0.50	100.0	0.0
No Code Yet	Communications & Cybersecurity (Draft)	Pio Fenton	Expert	5.0	3.00	3.00	100.0	0.0

Elective								
Mod Code	**Module Title**	**Co-ordinator**	**Level**	**Credits**	**FT Contact Hours**	**PT Contact Hours**	**Course Work**	**Formal Exam**
COMP9012	Applied Cryptography (Draft)	Donna OShea	Expert	5.0	3.00	3.00	100.0	0.0
MRKT9014	People Management Strategies (Draft)	Pio Fenton	Expert	5.0	2.00	2.00	40.0	60.0
COMP9071	Fraud and Anomaly Detection (Approved)	Donna OShea	Expert	5.0	4.00	4.00	100.0	0.0
No Code Yet	Emerging Cyber Trends (Draft)	Donna OShea	Advanced	5.0	3.00	3.00	100.0	0.0
FREE6001	Free Choice Module (Approved)	PAUL GALLAGHER	N/A	5.0	4.00	0.00	50.0	50.0

Stage 1 / Semester 3

Mandatory								
Mod Code	**Module Title**	**Co-ordinator**	**Level**	**Credits**	**FT Contact Hours**	**PT Contact Hours**	**Course Work**	**Formal Exam**
COMP9021	Computing Research Project (Draft)	Donna OShea	Expert	30.0	1.00	1.00	100.0	0.0

CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

APPENDIX 3 – PANEL TIMETABLE

Remote Validation Event for: **MSc in Cybersecurity Management**

Date: **Wed June 24th, 2020**
Modalities: **Teams Meeting**
Private Panel Meeting: Private Panel Meeting
Meeting with Programme Team: Meeting with Programme Team

Panel Timetable

Date / Time	Session
9.15 am - 9:45 am	Private Panel Meeting with Introduction from Registrar's Office
9:45 am - 11 am (1 hour 15 mins)	**1. Meeting with Programme Team - Programme Design** A short HoD presentation (max. 10 mins, e.g. PowerPoint) - Overall programme concept; intended graduate profile and typ. employment, links/efficiencies with other progs in School; staffing; resources & facilities. Discussion Points: **1.1** Is there a convincing need for the programme with a viable level of applications ? **1.2** Do the POs adequately describe the intended graduate profile, and align with the relevant award standard, incl. embedded target/exit award. **1.3** Is the learning experience of an appropriate level, standard and quality overall ? **1.4** Is the programme structure logical and well designed (including procedures for access, transfer, progression, derogation) **1.5** Are the programme management structures adequate ? **1.6** Are the resource requirements reasonable? **1.7** Will the impact of the programme on the Institute be positive? **1.8** Interim delivery arrangements due to Covid-19
11 am - 11:30 am	Private Panel Meeting plus break
11:30 am - 1 pm (1 hour 30 mins)	**2. Meeting with Programme Team - Programme Delivery** Discussion Points: **2.1** subject mix and thematic strands **2.2** delivery modes and teaching **2.3** learning & assessment strategy (Inc. any interim arrangements for remote delivery) **2.4** learning experience & supports **2.5** programme-critical modules as relevant (esp. final year theses/projects, placement, key specialist or prof. dev. modules).
1 pm - 2 pm	Private Panel Meeting plus lunch

2 pm - 3 pm (1 hour)	**3. Meeting with Programme Team - Programme Modules** **3.1** consideration of Module Review spreadsheet **3.2** individual module contents **3.3** semester assessment schedules
3 pm - 3:30 pm	Private Panel Meeting to progress report
3:30 pm - 3:45 pm	**4. Meeting with Programme Team - Feedback** Feedback to Programme Team