


| | | |
|-----|--|---|
| 1. | Title of Programme(s): (incl. Award Type and Specify Embedded Exit Awards) | MSc in Cybersecurity Operations Certificate in Cybersecurity Operations |
| 2. | NFQ Level(s)/ No. ECTS: | 9 Masters: 90 ECTS Certificate: 30 ECTS |
| 3. | Duration: | Masters: 2 years Certificate: 1 year |
| 4. | ISCED Code: | 0610 |
| 5. | School / Centre: | Mayo Campus |
| 6. | Department: | Department of Business, Humanities & Technology |
| 7. | Type of Review: | New Programme Validation |
| 8. | Date of Review: | 7 th December 2020 |
| 9. | Delivery Mode: | Online |
| 10. | Panel Members: | Dr Paul O’Leary, Head of Quality Promotion and Academic Policy Development, Waterford Institute of Technology Dr Trevor Prendergast, Head of Department of Accounting & Business Computing, Athlone Institute of Technology Dr Michael Schukat, School of Computer Science, NUI Galway Mr Tammo Oepkes, Information Security Manager, Doepke Schaltgeraete Ms Carmel Brennan, Assistant Registrar (Quality), GMIT (Secretary) |
| 11. | Proposing Staff: | Mr Michael Gill Dr Seamus Dowling Mr Brian Mulhern Mr Andrew Beatty Ms Noreen Henry Mr Mark Frain Dr Janine McGinn |
| 12. | Programme Rationale: | Businesses are acutely aware of the need to have cybersecurity measures in place and this programme aims to provide those businesses with the knowledge and means to address those concerns. An audit undertaken by the North West Regional Skills Forum in Collaboration with FIT (“The skills needs of the ICT and FinTech Sectors in the North West 2018”) identifies skills shortage |

| | | |
|-----|--|--|
| | | <p>nationally in InfoSec (IT security), IoT (internet of things), cyber security analyst, data/information security, and network security.</p> <p>Microsoft and Amarach Consulting in “Securing the Future 2020 – The state of Cybersecurity in Ireland” (2020) aims to “dispel the myth that security is an add-on, and start talking about security as a differentiator, money saver, and foundational element in every enterprise strategy.” The Galway Executive Skillnet Research Study (Walker, 2019) recommends the inclusion of Cyber Security as part of the flexible delivery options improving local access to continuing professional development.</p> |
| 13. | Potential Demand for Entry: | 24 students per annum |
| 14. | Stakeholder Engagement: | <p>This programme was developed in conjunction with Hewlett Packard Enterprises (HPE) Cyber Defense Center. Development meetings highlighted major skills shortages in cybersecurity and identified how GMIT could address these shortages. HPE collaborators identified cyber and security operations knowledge as essential skills for graduates and security personnel. HPE view cybersecurity as having a regional remit and want to collaborate with educational providers to realise this.</p> <p>An industry consultation session for the Mayo Campus in February 2020 also informed the programme, particularly the programme delivery mode. Cybersecurity experts in the region were also consulted and their advice influenced the content and structure of the programme.</p> |
| 15. | Graduate Demand: | The programme will provide new employment opportunities for graduates and opportunities for career progression for those who are already in employment in IT roles. Opportunities include roles in forensics, risk and compliance in non-core IT industries. |
| 16. | Entry Requirements, Access, Transfer & Progression: | <p>Minimum Entry Requirement: H2.1* in a Level 8 Degree or equivalent in IT/Computing or cognate area.</p> <p>Recognition of prior learning may be used as appropriate in line with the Institute’s policy on prior learning. Those deemed appropriately qualified for entry but with little evidence of research skills may be advised to undertake a Foundation in Research module prior to course commencement.</p> <p>Applicants whose first language/primary mode of expression is not English are required to produce evidence of English competence. An IELTS of Grade 6.0 (no section less than 6.0) is required.</p> <p>* This reflects the condition below relating to entry requirements.</p> |
| 17. | Programme Structure: | The masters programme consists of four 10 ECTS modules delivered on a yearlong basis during the first stage of the |

| | | |
|-----|---|--|
| | | <p>programme, with students being required to complete an applied research project in the second stage. The minor award which is a stand-alone qualification and acts as an exit award for the masters consists of three 10 ECTS modules delivered over one year.</p> |
| 18. | <p>Learning, Teaching & Assessment Strategies:</p> | <p>The teaching and learning strategy in this programme places learners at the centre of all interactions and engagement. Innovative online learning practices are facilitated to focus the learner's ability to discover, research, interact with peers and the lecturing team, and reflect on the outcome of these engagements. Lecturer-student engagement will be central to the development of an interactive community of learners and researchers, with contributions to content, generated not only by the lecturing team, but by students. This kind of participant interaction enables participants to gain maximum benefit from new knowledge generation in this discipline of Cybersecurity Operations. Learners will critically engage with each other and with the lecturing team to interrogate the topic of study, express opinions and listen to multiple points of view. The aim being to transform learning into a collaborative process, to co-create knowledge and provide solutions whilst remaining at the forefront in the rapidly evolving field of cybersecurity operations. Learners will be particularly encouraged to formally research and explore new technologies and techniques, and to deliver structured presentations on their findings and strategies in a student conference and interactive collaborative learning environment.</p> <p>The aim of the programme is to provide a potential avenue for graduate disciplinary conversion and/or continuing professional development and scholarly research practice, with a focus on those candidates already engaged in the workforce, and as such, a key tenet of the teaching and learning approach is to foster flexibility in the content delivery and learner engagement, whilst providing opportunities to foster an effective community of learners. Content will be made available online and learner community virtual interactions will be facilitated employing various virtual tools such as the VLE, live and recorded webinars, online discussion forums, polling tools, mobile apps, blogs, podcasting, social networks, sharing data and collaborative tools.</p> |
| 19. | <p>Resource Implications:</p> | <p>This programme will be self-financing. The Certificate programme is funded by Springboard+ this year.</p> <p>The programme can be delivered using existing staff resources. CPD has been identified which would benefit the lecturers on this programme.</p> <p>This programme requires a range of technical solutions to facilitate delivery and work is ongoing to ensure that virtual desktops, an IAAS platform and specialised online labs or similar solutions will be in place.</p> |

| | | |
|-----|--|--|
| | | |
| 20. | Synergies with Existing Programmes: | Students may benefit from cross-disciplinary research guest lecturers and share these with other programme research workshops. |
| 21. | Findings and Recommendations: | <p>General:</p> <p>The panel approve the programmes with the commendations (1) listed below and subject to the following condition(s) (4) and recommendation(s) (7):</p> <p>Commendations:</p> <p>The panel commended the programme developers on the following:</p> <ol style="list-style-type: none"> 1. The strong industry engagement which has informed the development of the programme. <p>Special conditions attaching to approval (if any):</p> <ol style="list-style-type: none"> 1. Amend the entry requirements for this programme to be a minimum of a H2.1 in a L8 major award or equivalent in IT/Computing or cognate area. 2. Review and modify the module learning outcomes for the 'Programming for Cybersecurity' module to ensure that they are written appropriately at level 9. Ensure there is a clear delineation between scripting and programming, with a stronger emphasis on scripting. 3. Normalisation of data (e.g. parsing, indexing, regular expressions) and integration between different security relevant tools (e.g. API programming) should be included in the 'Programming for Cybersecurity' module. 4. Review the module assessment strategy for the 'Secure Operations' module removing the 30% MCQ element. <p>Recommendations of the panel in relation to award sought:</p> <ol style="list-style-type: none"> 1. Rename the 'Secure Operations' module as 'Security Operations' to better reflect the content of the module. 2. Outline the weekly schedule that students will undertake, ensuring that it is manageable for students who may be working on a full-time basis. 3. Build industry partnerships to allow lecturers the opportunity to engage in shadowing or other relevant CPD opportunities. 4. Consider the use of capital expenditure rather than operational expenditure to ensure future operation of hands on laboratory work. 5. Review and amend the fourth and sixth module learning outcomes of 'Incident Detection and Response' ensuring they are clear and definitive. 6. Consider renaming the 'Dissertation/Formal Applied Project' module as 'Applied Research Project'. 7. In the entry requirements specify that IELTS scores cannot be below 6.0 in any individual element. |

| | | | |
|-----|------------------------|--|---|
| | | | |
| 22. | FAO: Academic Council: | Approved: | |
| | | Approved subject to recommended changes: | X |
| | | Not approved at this time: | |
| | Signed: | |  |
| | | Chair | Secretary |