VALIDATION REPORT

1.	Title of Programme(s): (incl. Award Type and Specify Embedded Exit Awards)	BSc in Cybersecurity (Level 7, 60 ECTS) Certificate in Data Cybersecurity (Level 7, 30 ECTS)
2.	NFQ Level(s)/ No. ECTS:	7 60 ECTS, 30 ECTS
3.	Duration:	BSc – 2 years part-time Certificate – 1 year part-time
4.	ISCED Code:	0610
5.	School / Centre:	Mayo Campus
6.	Department:	Department of Business, Humanities & Technology
7.	Type of Review:	External Panel
8.	Date of Review:	27th October 2020
9.	Delivery Mode:	Full-time, Online, Blended
10.	Panel Members:	Dr Terry Twomey, Registrar, Limerick IT (Chair) Mr Craig Andrews, Senior Penetration Tester, CMA Consulting, Toronto Mr Tom Davis, Information Technology Lecturer, School of Engineering and Information Technology, Limerick Institute of Technology. Mr Connor McEnroy, Cybersecurity Risk and Compliance Analyst, HP Enterprises, Galway Ms Carmel Brennan, Assistant Registrar (Quality), (Secretary)
11.	Proposing Staff:	Prof Neville McClenaghan Mr Michael Gill Mr Mark Frain Ms Noreen Henry Dr Seamus Dowling Mr Brian Mulhern Ms Clodagh Geraghty Dr Deirdre Garvey Ms Sinead Kilgannon Mr Pearce McDonnell
12.	Programme Rationale:	The programmes presented for validation are part of a suite of programmes in this discipline that have or are being developed to meet a recognised market need. The BSc award provides a progression pathway for students who have completed the Certificate in Network Cybersecurity which is currently being offered. National and international reports identify the

		importance of securing networks and information systems. The programmes aim to upskill IT practitioners in current tools and techniques to protect information at rest, in transit or processed for an organisation in line with industry best practices and in compliance with appropriate standards. IT and data security is widely required. Every organisation implements security measures at the network and operating system level to protect data from unauthorised access, disclosure, modification or destruction. It involves the planning, configuring and ongoing management of compliant network equipment and software to provide confidentiality, integrity, and availability to protect the network and data against malicious external and internal threats.
13.	Potential Demand for Entry:	24 students per annum
14.	Stakeholder Engagement:	The awards were developed in partnership with Hewlett Packard Enterprises (HPE) Cyber Defence Center. Development meetings highlighted major skills shortages in cybersecurity and identified how GMIT could address these shortages. HPE collaborators identified risk and compliance with project and operations knowledge as essential skills for graduates and security personnel. An industry consultation event was also conducted at the Mayo Campus with representation for diverse companies and organisations based in the county. In addition, industry leaders in Cybersecurity were contacted and meetings with these reviewed discussion documents and proposed programme structures.
15.	Graduate Demand:	There is strong evidence in the jobs market of availability of positions related to cybersecurity. This is backed up by evidence gleaned from stakeholder engagement.
16.	Entry Requirements, Access, Transfer & Progression:	Minimum entry requirement is a level 6 major award or equivalent. English language requirements are per GMIT code on Access, Transfer and Progression. RPL in line with GMIT policy can be used to gain access to or exemptions from the programme. Students may apply for progression to relevant cognate level 8 awards.
17.	Programme Structure:	The degree consists of a mixture of 5 and 10 ECTS module delivered on a semesterised basis. The Cybersecurity practical project offers learners the opportunity to amalgamate their skills, competencies and knowledge within the discipline and to apply their learning to an area of interest.
18.	Learning, Teaching & Assessment Strategies:	This programme will be delivered on a blended basis with attendance on campus one day per month approximately. The programme is also approved for online delivery which may be the mode of delivery during the current pandemic. A VLE will be used

		as the platform for delivering resources, engaging and communicating. Collaboration and interaction will be facilitated and encouraged. Assessment will be varied and appropriate to each module and will be scheduled in a student centred way.
19.	Resource Implications:	These programmes will be self-financing. 30 ECTS are already approved and funded through Springboard. No additional staff are required to deliver these programmes. Online and blended delivery requires an IAAS platform to facilitate remote access to lab equivalents. The approximate cost of this for 24 students would be €17,000. Specialised online labs are required to deliver these programmes, at an annual cost of €17,500. Resources required for the delivery of these programmes, other than staff costs, will be shared across a number of programmes (approved and seeking validation) in this discipline area. Staff upskilling will be required to ensure that staff stay up to date with this fast-moving discipline. It is proposed that four staff will engage in programmes through Sans.org costing in the region of €24,000. This will provide staff with knowledge and skills not only for the proposed programmes, but other programmes in this discipline area.
20.	Synergies with Existing Programmes:	30 ECTS of this programme is already approved as a Certificate in Network Cybersecurity, and both programmes can run in parallel with common teaching.
21.	Findings and Recommendations:	General: The panel approve the programmes with the commendations listed below and subject to the following condition(s) (0) and recommendation(s) (5): Commendations: Special conditions attaching to approval (if any): None

		Recommendations of the panel in relation to award sought:	
		1. Rename the degree award BSc in Network Cybersecurity to reflect the focus and content of the programme. Individual Modules: 2. LAN Cybersecurity – Include VLAN and VLAN Tagging within this module as part of port security. 3. Network Operating Systems Security – Include non-security flavours which are more enterprise focussed (e.g. Fedora, Ubuntu) rather than or in addition to the offensive security flavours listed i.e. Kali, Parrot. 4. Database Management – Explicitly reference NOSQL within this module. 5. Cloud Information Security - consider inclusion of assessment to evaluate students' practical knowledge in relation to this subject.	
22.	FAO: Academic Council:	Approved:	
		Approved subject to recommended changes:	X
		Not approved at this time:	
	Signed:		
		Chair	Secretary