



Programme Validation Report

Master of Science in Cybersecurity Management

<i>Version of Report</i>	<i>Author</i>	<i>Date</i>
1	Gráinne Hurley	20/03/2025
2.	Gráinne Hurley	27/03/2025
		Click or tap to enter a date.
		Click or tap to enter a date.

<i>Approval</i>	<i>Date</i>
Programme Proposal approved by Faculty Board	06/02/2025
Programme Proposal approved by University Programmes Board	11/02/2025
Programme approved by Faculty Board	Click or tap to enter a date.
Programme approved by University Programmes Board	Click or tap to enter a date.

Section A - Programme Details

Title	Master of Science in Cybersecurity Management
NFQ Level	9
ECTS Credits	90
Mode of delivery	Part-time <input type="checkbox"/> Full-time <input checked="" type="checkbox"/>
Duration	Part-time: Full-time: 12 months
Mode of provision	Face-to-Face <input checked="" type="checkbox"/> Blended <input type="checkbox"/> Online <input checked="" type="checkbox"/>
Classification of award	First Class Honours; Second Class Honours, Upper Division; Second Class Honours, Lower Division; Pass (See Section F below)
Discipline Programmes Board	Cybersecurity, and Management, People, and Organisations
Faculty Board	Faculty of Computing
Schools involved in delivery	Cybersecurity, and Management, People, and Organisations
Delivery location	Blanchardstown and Aungier Street
Collaborative Partner (where applicable)	
Date of Commencement	

Section B - Awards

Award Title	Master of Science in Cybersecurity Management
NFQ Level	9
Award Class	Major
ECTS Credits	90
Classification of award	1 st Class Honours; 2nd Class Honours, Upper Division; 2nd Class Honours, Lower Division; Pass (See Section F below)
Award (1) Title	Postgraduate Diploma in Cybersecurity Management
Exit/Embedded	Exit <input checked="" type="checkbox"/> Embedded <input type="checkbox"/>
NFQ Level	9
Award Class	Major
ECTS Credits	60
Classification of award	Distinction; Merit Grade 1; Merit Grade 2; Pass
Exit Award (2)	Postgraduate Certificate in Cybersecurity
Exit/Embedded	Exit <input checked="" type="checkbox"/> Embedded <input type="checkbox"/>
NFQ Level	9
Award Class	Minor
ECTS Credits	30
Classification of award	Distinction; Merit Grade 1; Merit Grade 2; Pass
Exit Award (3)	Postgraduate Certificate in Management
Exit/Embedded	Exit <input checked="" type="checkbox"/> Embedded <input type="checkbox"/>
NFQ Level	9
Award Class	Minor
ECTS Credits	30
Classification of award	Distinction; Merit Grade 1; Merit Grade 2; Pass

Section C - Programme Derogations (if required)

<i>Derogations from Assessment Regulations/Marks and Standards already approved by University Programmes Board</i>	
Date of University Programmes Board Approval	Click or tap to enter a date.

Section D Validation Process

Please tick the process that was followed:

Validation Panel <input checked="" type="checkbox"/>	AQEC Meeting <input type="checkbox"/>	AQEC Sub-Group <input type="checkbox"/>
Date: 11 March 2025	Date:	Date:

Panel Members

Name	Role	Affiliation
Dr Fiona Murray	Chairperson	Head of Discipline, Applied Probability, Statistics & Data Analysis at the School of Mathematics
Dr Lubna Luxmi Dhirani	External Panel Member	Assistant Professor, Department of Electronic & Computer Engineering, University of Limerick
Paul O'Reilly	Internal Panel Member,	GROWTHhub Project Lead, TU Dublin
Shaun Ferns	Internal Panel Member	University Education Model Lead, Office of the Registrar
Dr Gráinne Hurley	Secretary to the panel/Academic Quality Advisor	Quality Framework, Academic Affairs

Section E - Programme Evaluation

Governance & Management		
<i>Is the programme designed in accordance with the University's Strategic Plan, Educational Model and Quality Framework?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
<p>Comment:</p> <p>The M.Sc. in Cybersecurity Management strongly aligns with TU Dublin's Strategic Plan under the three key pillars as outlined below:</p> <p>People: The programme develops future-ready leaders by combining expertise from the School of Informatics and Cybersecurity and the School of Management, People & Organisations. It fosters talent through interdisciplinary collaboration, equipping graduates with the skills needed for leadership roles in the cybersecurity industry.</p> <p>Planet: By embedding sustainability and ethical considerations into its design, the programme aligns with TU Dublin's focus on addressing global challenges and ensuring long-term resilience in cybersecurity and business practices.</p> <p>Partnership: Designed with input from both disciplines and continuous engagement with industry stakeholders, the programme reflects real-world needs and ensures graduates are prepared to address evolving challenges. Its delivery by both schools reinforces collaboration and innovation.</p> <p>Graduate Attributes (Graduate Attributes have been mapped to programme modules in Table 18 (p. 48) of the validation document).</p> <p>GA/01 People</p> <p>Digitally capable, life-long learners:</p> <p>The M.Sc. in Cybersecurity Management equips graduates with the digital capabilities and adaptability needed to thrive in the rapidly evolving cybersecurity landscape. The programme's blended learning approach fosters lifelong learning, enabling students to continuously upskill in response to emerging threats, technologies, and industry best practices. Modules such as Cybersecurity Theory and Strategy, AI for Cybersecurity Management, and Enterprise Security Architecture ensure that graduates are well-versed in cutting-edge digital tools and cybersecurity frameworks. Additionally, the emphasis on strategic leadership and decision-making prepares</p>		

students to navigate complex digital transformations, making them resilient and proactive professionals in an ever-changing technological environment.

By integrating real-world case studies, industry-led projects, and applied research, the programme also encourages students to develop a growth mindset, empowering them to adapt to new challenges beyond the classroom. The opportunity to engage with cybersecurity labs, simulations, and collaborative exercises further enhances their ability to harness digital tools effectively in professional settings. These experiences foster critical thinking, digital literacy, and the agility required to lead cybersecurity initiatives in a globally connected world.

GA/02 Planet

Sustainability-focused, global citizens

The Faculty of Computing, Digital and Data has documented in video form much of the work that it is doing towards the achievement of the Sustainable Development Goals, as part of its Tech-Ed for Good Series. These resources will be promoted to the students on the M.Sc. in Cybersecurity Management as they are for all students in the Faculty of Computing, Digital and Data. Cybersecurity plays a crucial role in ensuring the sustainability and resilience of digital infrastructures, and this programme integrates sustainability principles into both its curriculum and learning ethos. The M.Sc. emphasises ethical cybersecurity leadership, preparing graduates to make responsible and equitable decisions that align with the evolving regulatory and sustainability landscape. Modules such as Cybersecurity Resilience, Compliance, and Ethics address the importance of compliance, responsible data governance, and ethical cybersecurity practices, ensuring that graduates contribute to a more secure and sustainable digital world. Additionally, students will have access to TU Dublin's Tech-Ed for Good Series, which showcases initiatives aligned with the United Nations Sustainable Development Goals (SDGs). By promoting these resources, the programme encourages students to consider the broader societal impact of cybersecurity, including issues such as digital inclusion, data privacy, environmental sustainability in tech, and cyber resilience in critical infrastructure sectors. Through applied research projects, students will also have the opportunity to develop cybersecurity strategies that address sustainability challenges, reinforcing their role as socially responsible global citizens. See Table 11, (p. 31) of the validation document.

GA/03 Partnership

Collaborative, real-world problem solvers

The M.Sc. in Cybersecurity Management is rooted in industry collaboration and real-world problem-solving, ensuring that graduates are equipped with practical skills to tackle cybersecurity challenges in diverse sectors. The programme has been developed through ongoing consultation with industry stakeholders, including Workday, Expel, Liberty IT, and ReliaQuest, to ensure that its learning outcomes are aligned with industry needs. Collaboration is embedded within the programme's interdisciplinary approach, which brings together Computing, Digital and Data and Business faculties to bridge the gap between technical expertise and strategic leadership. The programme structure ensures that students from diverse backgrounds work together, fostering cross-disciplinary problem-solving and teamwork. Additionally, the use of the Blanchardstown Campus Cybersecurity Training SOC (Collaboratory) will provide a unique experiential learning opportunity, where students will gain hands-on experience in cybersecurity operations and leadership. By embedding collaborative, project-based learning, the M.Sc. ensures that graduates are confident, proactive, and effective problem solvers, ready to take on leadership roles in cybersecurity.

Programme Alignment with the UEM

The programme integrates with the UEM principles, as highlighted below. See also Table 10 (p. 30) of the validation document for a mapping of the programme to UEM Principles):

1. Learner-Centred Education

- a) The M.Sc. uses authentic assessments such as real-world cybersecurity case studies, industry projects, and cyber-attack simulations, ensuring a practice-oriented learning experience.
- b) Flexible learning pathways are supported through embedded awards, where students can exit with a 30-credit certificate, a 60-credit diploma, or a 90-credit M.Sc. Students will also have a choice of elective modules in semester 1 and semester 2, including a free elective in semester 2.
- c) The curriculum is highly applied, with guest lectures from industry leaders, engagement with cybersecurity competitions, and the integration of work-based learning.

2. Interdisciplinary Engagement

- a) The programme is co-delivered by the School of Informatics and Cybersecurity and the School of Management, People and Organisations, ensuring a balanced mix of cybersecurity knowledge and strategic leadership.
- b) Modules integrate cybersecurity, governance, finance, and leadership, reflecting the interdisciplinary nature of modern cybersecurity roles.

3. Digital Inclusion and Sustainability

- a) Learning outcomes map to United Nations Sustainable Development Goals (SDGs), particularly SDG 4 (Quality Education) and SDG 16 (Peace, Justice, and Strong Institutions) by promoting cybersecurity awareness and resilience. Table 9 labels each module learning outcome as Sustainability Focused, Sustainability Inclusive, or Neither.
- b) Diversity and inclusion are actively promoted through engagement with international students, gender diversity initiatives (e.g., Women in Tech networks), and accessibility considerations in module design and assessment.

The programme validation document demonstrates that the programme aligns to the 7 Fundamentals of the UEM, as outlined below. Please refer to Table 9 (p. 28) of the validation document:

Fundamental 1

The programme team/Schools are committed to streamlining existing modules as per 'Action Fundamental 1', for example reusing existing modules.

- All modules from the School of Management, People and Organisations are delivered on existing programmes, except the Strategic Risk and Crisis Management module. This is new but will be shared with other M.Sc. programmes when developed.
- The research project module is shared with TU252R the M.Sc. in Applied Cybersecurity.
- The cybersecurity electives are 5 credit versions of the existing modules on TU252R, or a free elective.

Fundamental 2

The Schools involved are committed to validating modules in an online and in-person mode. This modality has been added on Akari for all new modules. The School of School of Management, People & Organisations commit to updating existing modules to contain a two modalities: online and in-person.

Fundamental 3

This programme is a progression opportunity from all undergraduate programmes in Science, Computing, Maths, Engineering, and Business.

Fundamental 4

The programme includes an elective in each semester, with the potential for a free elective in semester 2. However, the timeline for the technological systems to support its implementation

remains uncertain. Given the programme's condensed structure and multidisciplinary approach, an initial limit of 5 credits for the free elective was applied.

Fundamental 5

The inclusion of the Framework is clear throughout the programme report. Given that this programme is at least half a computing discipline, all assessments, except final written exams and some In-class tests in the Finance modules, are digital. When a learning agreement is in place, supports such as extended time, different settings (e.g., quieter rooms) or the presence of aids (note-takers, sign language interpreters) may be offered to help students demonstrate their true competencies, to ensure that all assessments are inclusive. All assessments test theoretical and practical knowledge and skills and, therefore, can be viewed as authentic.

Fundamental 6

Students will engage with their peers in programmes such as TU252R, TU5352, TU252_PGD, TU309, and TU421, through shared modules and group work assessment. The free elective in semester 2 provides further opportunity for engagement beyond the programmes listed above.

Fundamental 7

One of the main objectives of the Cybersecurity Management is related to sustainability. Tables 16 and 17 (pp. 45 & 46) of the validation document detail the mapping of the modules to the programme learning outcomes. PLO 8 is related to sustainability. Section 6.8 details a more granular view of sustainability across the programme. Table 11 (p. 31) shows the classification of each module learning outcome according to the scheme (Sustainability-focused; sustainability-inclusive or neither).

The School operates in accordance with the TU Dublin Quality Assurance and Enhancement processes.

The panel commended the impressive alignment to Graduate Attributes at programme level and that the sustainability engagement was exemplary.

<i>Will the proposed strategies for programme management and quality assurance ensure that the programme is well managed and continuously enhanced and is in accordance with the University's Quality Framework?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
--	---	-----------------------------

Comment:

The programme will be managed by Discipline Programme Boards. Each Discipline Programmes Board is a sub-committee of Faculty Board and fulfils academic responsibilities within the framework laid down by Academic Council as specified in the TU Dublin Quality Enhancement Framework. As part of the Quality Framework, there is a requirement for all programmes to implement a Programme Team comprised of all teaching staff involved in the programme, and to assign a Programme Coordinator who assumes overall responsibility for the management of quality assurance on the programme. For the M.Sc. in Cybersecurity Management, an overall Programme Coordinator will be assigned by the School of Cybersecurity and additional Programme Coordinators will be assigned by the School of Management, People and Organisations. The overall Programme Team and sub-teams for each specialism will meet as per the requirements of the Quality Framework on at least two occasions each academic year. The M.Sc. in Cybersecurity Management will report to the Cybersecurity and Management and Leadership Discipline Programme Board.

Given that this is a shared programme, the panel stressed the need for regular meetings between the two disciplines within the development team in order to facilitate alignment and that they consider proper and balanced representation of the programme team and opportunities for socialisation of staff and sharing of knowledge. This should be addressed before students are recruited (see Recommendation no. 4).

Awards Standards		
Are the programme aims and learning outcomes clearly written using appropriate terminology? (See TU Dublin Guidelines)	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
Comment:		
Are the programme aims and learning outcomes aligned to the proposed level of the award on the NFQ in accordance with applicable Award Standards?	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
Comment:		
Will the curricula, teaching, learning and assessment methods enable students to reach the appropriate standard to qualify for the award(s)?	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
<p>Comment:</p> <p>The University has a dedicated Learning, Teaching and Assessment team, which works closely with academic staff to bring a commitment of research-informed teaching that promotes a programme-based culture and helps to create a quality inclusive learning experience for all students. The team offers a range of academic development opportunities for staff who teach, including events and workshops, consultative support, and accredited and non-accredited postgraduate CPD modules and programmes. In addition, the Faculty's Head of Learning Development (role currently unfilled) organises regular lunch time symposiums on examples of good teaching and learning practice happening in across the faculty, covering themes such as AI in the classroom, creative coding, building sustainability into programmes, incorporating soft skills in a technical programme and many more. Recordings are available on the Faculty's intranet.</p> <p>This programme and its modules benefit from a wide range of teaching strategies in order to motivate the students to engage and obtain as much from the planned learning events as possible. Each module leader has the flexibility to apply their own strategies to learning and teaching. The various methods are contained in the module descriptors for each module which accompanies this document.</p> <p>A range of technologies are used to support learning and teaching and the Virtual Learning Environment (VLE) forms a core component of all module delivery in terms of provision of notes, supporting reading and reference materials, discussion boards, assessment and feedback.</p> <p>Assessment strategy and schedule</p> <p>A variety of teaching and learning methods are employed on the programme including lectures, problem-based learning, online support, group projects, and guest lectures which are detailed in the accompanying module descriptors. Assessment is part of learning and is an integral part of programme planning. Assessment is designed to be beneficial in its effect, particularly in motivating students and is used to measure the intended module learning outcomes. Students are made aware of all information relevant to the assessments including the criteria by which they are graded.</p> <p>Many modules in the programme include weekly graded lab work so students are getting frequent feedback on how they are progressing. As student progress, there are more opportunities for self-directed learning and completion of more complex assessment briefs over several weeks. This is in addition to workplace learning and learning undertaken as part of taught modules. Integration between modules is encourage through combined assessment briefs, projects, and in class discussions.</p>		

<p>In keeping with the terms of the TU Dublin Student Charter students are provided with a schedule of assignments for each module in the first two weeks of the academic semester. By using assessment schedules, the programme team can review the workload of the students and spread the coursework across a number of weeks to avoid congestion in the student workload. There are also several resources on the TU Dublin website for all stakeholders (see here). An Epigeum training module on Academic Integrity, developed for new students, is available on all of TU Dublin's VLE instances.</p> <p>Academic integrity is critical to the reputation of higher education, including the recognition of the graduate's academic learning and qualifications. It can be defined as <i>"compliance with ethical and professional principles, standards, practices and consistent system of values, that serves as guidance for making decisions and taking actions in education, research and scholarship"</i> as defined by Quality and Qualifications Ireland.</p> <p>The panel thought it would be beneficial to develop a programme development plan across all of the modules to integrate the two aspects of the programme.</p>		
<p><i>Was the programme development appropriately informed by internal and external stakeholder input (including industry/practice, professional/regulatory bodies, and community organisations)?</i></p>	<p>Yes <input checked="" type="checkbox"/></p>	<p>No <input type="checkbox"/></p>
<p>Comment:</p> <p>A comprehensive survey process was conducted. This involved gathering insights from current students in senior stages of cybersecurity programmes, as well as industry professionals working in cybersecurity. The student survey focused on interest in the programme, familiarity with leadership roles and desired career progression, while the industry survey examined employer demand, skill gaps, and the relevance of the proposed curriculum. The findings from these surveys played a crucial role in shaping the programme's structure, ensuring that it develops graduates with the necessary mix of technical expertise and management skills. During the initial phase of the programme review, feedback from a group of cybersecurity industry stakeholders was sought on the programme's overall structure (see p. 14 of validation document for responses). To complement the survey findings and gain deeper insights, two one-hour focus groups with industry stakeholders were conducted. Each session consisted of small groups of two participants and a facilitator. Industry representatives from Workday, Expel, Liberty IT, and ReliaQuest participated in the discussions. An overview of the programme structure and modules was presented (and provided in advance), followed by a structured discussion covering key questions. The meetings were recorded, and transcripts were later analysed to extract valuable insights.</p> <p>The panel appreciated the extensive consultation with industry and students but it felt that some aspects of the feedback were not reflected in the programme design (see Recommendation no. 8)</p>		
<p><i>Has the programme been benchmarked against similar programmes nationally and internationally?</i></p>	<p>Yes <input checked="" type="checkbox"/></p>	<p>No <input type="checkbox"/></p>
<p>Comment:</p> <p>Several universities offer similar M.Sc. programmes, each with a unique focus on cybersecurity risk, compliance, and governance, notably the M.Sc. in Cybersecurity Risk Management at the University of Galway; the M.Sc. in Cybersecurity Management at Munster Technological University, and the M.Sc. in Cyber Risk for Business at University College Cork (the core and elective modules of each are provided in Table 3 (p. 9) of the validation document). This proposed programme differentiates itself from these programmes through several key competitive advantages (illustrated in Table 4 (p. 11) of the validation document).</p>		


<i>Did the programme development take account of relevant external discipline benchmarks and Professional Statutory and Regulatory Body requirements?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
Comment:		

Programme Design		
<i>Is the programme design informed by current development in the discipline and associated subject areas, having taken into consideration current trends, stakeholder feedback and market analysis?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
<p>Comment:</p> <p>The M.Sc. in Cybersecurity Management has been developed in response to the increasing demand for cybersecurity professionals who can effectively bridge the gap between technical expertise and strategic leadership. As cyber threats become more sophisticated, organisations require skilled managers who can implement robust cybersecurity frameworks, navigate regulatory landscapes, and align security strategies with business objectives. This programme, designed and delivered jointly by the School of Informatics and Cybersecurity and the School of Management, People and Organisations, is designed to equip graduates with a unique blend of cybersecurity knowledge and leadership skills to address these challenges.</p> <p>The development of the M.Sc. in Cybersecurity Management followed a structured and consultative process, ensuring that internal and external perspectives were incorporated into the programme design. The development team conducted a literature review to assess cybersecurity leadership trends and skill gaps. The programme was informed by the Cyber Labour Market Report 2023, which highlighted a tripling demand for cybersecurity talent in Ireland; the EU Cybersecurity Skills Academy, which emphasised the European-wide shortage of cybersecurity professionals, and the NIST NICE Framework, ensuring alignment with internationally recognised cybersecurity competency areas. A LinkedIn job market analysis was carried out to identify employer demand for cybersecurity managers.</p> <p>The programme takes a management-oriented approach to cybersecurity, focusing on governance, risk management, policy development, and strategic decision-making rather than purely technical implementations. By integrating cybersecurity principles with business management, the M.Sc. prepares students for leadership roles where they can influence cybersecurity strategy, manage organisational risk, and ensure resilience against cyber incidents. The curriculum is informed by international frameworks, specifically the NIST NICE Framework, and has been developed in consultation with industry stakeholders to ensure its relevance to real-world needs. The M.Sc. in Cybersecurity Management is rooted in industry collaboration and real-world problem-solving, ensuring that graduates are equipped with practical skills to tackle cybersecurity challenges in diverse sectors. The programme has been developed through ongoing consultation with industry stakeholders, including Workday, Expel, Liberty IT, and ReliaQuest, to ensure that its learning outcomes are aligned with industry needs. In addition, there were programme meetings and internal consultation.</p> <p>The panel felt that some of the modules on offer did not fully reflect the stakeholder feedback and to this end it strongly recommended that the programme development team reconsider the core Management modules on offer (see Recommendation no. 5).</p>		
<i>Will there be opportunities for students to input into curriculum design decisions in the future?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
Comment:		

The student voice plays an essential role in the TU Dublin Quality Assurance and Quality Enhancement processes and procedures.		
<i>Is there a mechanism to ensure the input of external stakeholders in the ongoing development of the programme?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
<p>Comment:</p> <p>Many academic staff members belong to the Dublin Chapter of Cyber Ireland, a national cyber security cluster organisation that includes industry, academia, and government representatives to address the needs of Ireland's cyber security ecosystem. The school has well-established partnerships with companies like Orange, Microsoft, and Workday. It also maintains a robust network of cybersecurity graduates active in the Irish cybersecurity industry, engaging with them through research proposals (such as CommSec and TU ARISE), invited talks, sponsorship of CTFs (e.g., EdgeScan and ReliaQuest), field trips (including visits to Ecko and ReliaQuest), and industry sessions (with companies like Ward Solutions, EdgeScan, and IBM).</p> <p>The School of Management, People and Organisation has an established Industry Advisory Board (IAB), which to strengthens its engagement with industry and ensures that its programmes align with current and future business needs. The IAB serves as a vital link between academia and industry, providing strategic guidance and insights into emerging trends. Comprising distinguished professionals from various sectors, including John McManus (Country Director, Advanced), Lorraine Toole (Director, Talent Acquisition at Workday), and Natasha Kinsella (Dublin Regional Skills Forum Manager), the board offers diverse perspectives to inform the School's curriculum and activities. Through collaborative discussions, the IAB assists the School in identifying the 21st-century skills required by graduates, thereby enhancing employability and ensuring that educational offerings remain relevant in a rapidly evolving business landscape. This partnership underscores the School's commitment to fostering meaningful connections with industry, professional bodies, and the community to drive positive change and prepare students for future challenges</p>		
<i>Is the programme curriculum well-structured with a logical progression of learning and development across the modules and stages?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
<p>Comment:</p> <p>Given the fast-moving cybersecurity landscape, the panel recommended that consideration should be given to broadening elective opportunities, particularly in industry, in areas such as Innovation Management, Project Management, and Entrepreneurship.</p>		

<i>Are there appropriate opportunities for students to undertake work-based learning, through work placements or work-based projects or assignments?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
<p>Comment:</p> <p>Students are encouraged to engage with an industry partner for projects, and some industry-based projects are also sourced by staff.</p> <p>ReliaQuest and Ecko have become an invaluable component of the educational journey for the cybersecurity students. These visits offer a firsthand look at the inner workings of the industry, bridging the gap between theoretical knowledge and practical application. Additionally, the invited speakers from the cybersecurity and Management fields enrich the learning experience by providing students with insights into the latest trends, challenges, and opportunities in cybersecurity and Management. Industry sessions are organised every year where the School invites companies interested in hiring graduates to speak to the students, ensuring that students have a chance to network and are aware of the opportunities that exist. The Blanchardstown campus also run an annual careers fair.</p> <p>The newly opened Collaboratory at TU Dublin will also provide opportunities for students and academics to collaborate with relevant industry partners in the context of awareness education/training and research and innovation.</p>		
<i>If applicable, have the relevant Blended Learning Checklists (i.e. Learning Experience Context & Programme Context) been fully completed and submitted to the Panel?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
<p>Comment:</p> <p>The panel made it a condition for approved modes of delivery to be accurately recorded and that modalities for each module must be clearly identified. The panel recommended that modules should be validated in at least 2 modalities and to consider the 4 approved modalities for flexibility. It also recommended that the Schools consult and consider incorporating QQI Guidelines on blended learning.</p>		
<i>Is the required programme and module information provided in the correct format?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
<p>Comment:</p>		

Learning, Teaching & Assessment		
<i>Is there an effective student-centred teaching and learning strategy that aligns with the University's strategies and Education Model?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
<p>Comment:</p> <p>TU Dublin's UEM strives to achieve these objectives by means of 10 guiding principles. The programme is underpinned by these ten principles, exemplified as follows and explored in subsequent sections:</p> <p>1) Student-centred and student-engaged learning by providing opportunity for individual and team work to foster collaboration, use of authentic assessments, and offering elective modules to support learner agency.</p> <p>2) Connected, engaged, internationalised curriculum with a strong emphasis on the application of knowledge, research, ethics and sustainability for the common good.</p> <p>3) Diversity of provision and focus on practice and career development.</p> <p>4) Excellent, flexible agile teaching and learning: authentic assessments use of range of technologies to support teaching, learning and assessment; and experiences of multi-modal delivery.</p> <p>5) Knowledge creation to application: including workplace learning via guest lecturers and an applied learning experience.</p> <p>6) A highly engaged student experience through active learning and engagement embedded throughout the programme and a choice of elective modules.</p> <p>7) Inclusive, global, multicultural: Dublin 15 boasts Ireland's most racially diverse population that is reflected in the student cohort. The school also has a strong international student enrolment and a very active Women In Technology network. The academic staff in the School of Informatics and Cybersecurity is composed of 32% females, and 18% of the total staff are from outside Ireland.</p> <p>8) Continuous developing, committed and caring staff: the industry-relevant and applied research undertaken by the programme team informs the continuous development of programmes.</p> <p>9) Transition is supported by an extended student induction and ongoing support upon enrolment on all programmes.</p> <p>10) Access and equal opportunity: Recognition of Prior Learning (RPL) is included in all programme entry criteria, along with a culture that fosters equality.</p>		
<i>Does the assessment strategy provide an appropriate mix of assessment types that will enable students to demonstrate that they have met the module and programme learning outcomes?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
<p>Comment:</p> <p>The panel recommended that transversal skills be added to PLOs (see Recommendation no. 5). Given that cybersecurity is a fast-moving landscape, that panel felt that consideration should be given to broadening elective opportunities, particularly in industry, in areas such as Innovation Management; Project Management, and Entrepreneurship (see Recommendation no. 9).</p>		

<i>Do the learning outcomes and assessment strategy ensure that academic integrity can be maintained and attempted breaches of academic integrity are minimised/easily detected?</i>	Yes ✓	No <input type="checkbox"/>
Comment: All students who gain access to the university VLE have to agree to undertake Epigeum training on Academic Integrity.		
<i>Is there a comprehensive mapping of assessment methods and module learning outcomes and between module learning outcomes and programme learning outcomes?</i>	Yes ✓	No <input type="checkbox"/>
Comment: The mapping of Programme Learning Outcomes to Module Learning Outcomes is provided in Tables 16 & 17 (pp. 45 & 46 of the validation document). The panel advised that any free electives must be mapped to PLOs.		
<i>Are there opportunities in all modules to provide students with timely and constructive feedback on their learning and development?</i>	Yes 	No <input type="checkbox"/>
Comment: Timely feedback is provided on all assessments in order that students can identify areas that have been completed satisfactorily and clearly know which sections require further study. Students can expect the return of marked assignments with feedback within two weeks. All feedback will be designed to achieve its intended purpose, as highlighted below: <ul style="list-style-type: none"> • summative - providing an accurate judgement and record of a student's attainment • formative - helping a student to learn from previous performance in order to improve • diagnostic - ascertaining students' strengths, learning or developmental needs Each module leader is responsible for the type and approach taken to feedback. The vast majority of personalised feedback is provided through the VLE. Here, lecturers can comment, grade and provide detailed feedback which can be made available to the students to view online. Generalised feedback is also given during scheduled classes.		
<i>Do the teaching and assessment methods consider the diversity of the student cohort?</i>	Yes ✓	No <input type="checkbox"/>
Comment:		

Student Supports & Learning Environment		
<i>Are there sufficient and appropriate resources (e.g. human, financial and physical) to support the proposed programme aims and objectives, to deliver the programme as specified?</i>	Yes ✓	No <input type="checkbox"/>
Comment:		
<i>Are there sufficient staff that are appropriately qualified and capable to support the programme delivery, from both context and pedagogy perspectives?</i>	Yes ✓	No <input type="checkbox"/>
Comment:		
<i>Are there appropriate arrangements in place to support the student experience and to monitor student performance?</i>	Yes ✓	No <input type="checkbox"/>
Comment:		

This programme is designed to actively support student engagement and success through a range of academic, professional, and well-being initiatives that enhance learning, development, and career readiness, as outlined below.

Induction/orientation programme

Dedicated student orientation programmes are provided at the start of the academic year, organised by the faculty's Head of Learning Development, Heads of Discipline, Programme coordinators and the year tutors for new students. The programme's academic team meet with the students to run icebreaker sessions and explain their subject areas. Students also get an introductory lab session to make sure each student can log in and knows how to access their timetables and virtual learning environment in advance of their first class. Additional presentations from support staff, IT staff, library staff and other supports are provided during the orientation session and students are provided with a copy of the Student Handbook. Students are also taken on a guided tour of the campus. The faculty runs an Extended Induction programme enabling students to learn about the supports and services available to them in Higher Education and acquire some of the knowledge and skills required to be successful in their studies. Importantly, and unlike an Orientation programme, Extended Induction takes place over the first 4-7 weeks that a student is studying on their programme in Higher Education. An Extended Induction programme was developed to meet the needs of its new students while making effective use of digital technology to engage and empower all participants. Students receive a badge once all activities are completed.

Peer engagement sessions are run each semester where new students can talk with trained peer mentors, provided by the school. The activity is currently run collaboratively across all schools that are running programmes on the Blanchardstown campus, and co-ordinated by the chaplaincy.

The panel felt it important for the Programme Development team to provide students with a seamless, integrated and cohesive experience (e.g. joint extended induction/orientation; coherence across assessment approaches/schedules and the research project). See Recommendation no. 3. The panel recommended that there should be proper representation of the programme team and opportunities for socialisation of staff and sharing of knowledge which will facilitate this cohesion and alignment (see Recommendation no. 4).

<i>Are the access, transfer and progression arrangements clearly defined and appropriate, and aligned to TU Dublin policy/strategy in this regard?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
--	---	-----------------------------

Comment:

The panel recommended that the programme information makes it clear that it is a conversion programme.

<i>Do the student supports and learning environment cater for equality, diversity and inclusivity of students?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
--	---	-----------------------------

Comment:

The M.Sc. in Cybersecurity Management is committed to Equity, Diversity, and Inclusion (EDI), ensuring that all students, regardless of background, have equitable access to learning, support, and professional development opportunities. The programme aligns with TU Dublin's EDI Strategy and incorporates Universal Design for Learning (UDL) principles in its teaching, assessment, and learner support mechanisms to create an inclusive and accessible learning environment.

EDI in Programme Design and Delivery

- The blended learning approach accommodates students with diverse learning needs, including those balancing work, family, or accessibility requirements. Live, recorded, and asynchronous content ensures flexibility and accessibility.

- Module content incorporates global perspectives on cybersecurity governance, ethical AI, and digital inclusion, addressing EDI challenges within cybersecurity leadership. Topics such as bias in AI, inclusive cybersecurity policies, and ethical hacking frameworks ensure diverse viewpoints are explored.
- Case studies and examples draw from a wide range of international cybersecurity contexts, ensuring students engage with different regulatory environments, cultural considerations, and ethical dilemmas in cybersecurity.
- The programme ensures digital accessibility by providing materials in multiple formats, including text, video with captions, and screen-reader-friendly resources.

EDI in Teaching and Assessment (Universal Design for Learning - UDL)

Multiple Means of Engagement:

- Assessments offer varied formats, including written reports, video presentations, case studies, and interactive simulations, allowing students to demonstrate learning in diverse ways.
- Interactive and collaborative learning environments, such as team-based cybersecurity challenges and problem-solving exercises, encourage peer learning and inclusion.

Multiple Means of Representation:

- Recorded and captioned lectures, digital labs, and structured self-paced materials support students with different learning preferences and accessibility needs.
- Use of real-world cybersecurity case studies featuring diverse industries, organisations, and cultural contexts.

Multiple Means of Action & Expression:

- The programme allows students to develop tailored cybersecurity management projects that align with their professional interests and experiences.
- Formative feedback and reflection exercises ensure continuous learning without disproportionately disadvantaging students unfamiliar with academic conventions.

Support for Diverse Learners:

- Students have access to TU Dublin's Disability Support Services, Learning Development Centre, and Career Services, ensuring they receive guidance tailored to their needs.
- Industry engagement incorporates diverse guest speakers, including underrepresented voices in cybersecurity, fostering an inclusive professional network.
- The programme encourages applications from students of varied backgrounds, particularly those from underrepresented groups in cybersecurity. Outreach efforts ensure visibility and accessibility to a broad student base.

<i>Is the relevant programme information clearly communicated to the students to ensure they are informed, guided and cared for?</i>	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
Comment: This information is provided in the Student Handbook.		
<i>Has the Checklist for First Year Student Success (where applicable) been fully completed and submitted to the Panel?</i>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Comment:		

Collaborative Provision (if applicable)

<i>Are the roles and responsibilities of each partner clearly defined?</i>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Comment:		

In the case of Joint or Multiple Awards, has due diligence on capacity of partner institution meeting the QA-QE requirements for the programme been undertaken?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
Comment:		

Section F - Overall Recommendation

1.	Recommend approval of programme as submitted, without amendment	<input type="checkbox"/>
2.	Recommend approval of programme, subject to minor amendments/editorial changes to be completed as soon as possible and with recommendations for consideration. Note: recommendations are attached where it is considered that the programme would benefit from particular changes, or from a review of certain aspects of the programme over a period of time, with changes made if required. While recommendations are advisory in nature, there is an expectation that all recommendations are responded to appropriately and acted upon as appropriate.	<input type="checkbox"/>
3.	Recommend approval of programme subject to the fulfilment of conditions. Recommendations for consideration may also be attached. Note: conditions are attached where it is agreed that changes must be made to the programme / programme documentation prior to the commencement of the programme. Conditions must be set where issues are identified that relate directly to academic standards or to University regulations or procedures. It should be clear what is required in order to meet the conditions. A new programme cannot go forward to Faculty Board for consideration/approval unless a response to the Validation Report is submitted with revised programme documentation and the Academic Quality Enhancement Committee is satisfied that all conditions are met.	<input checked="" type="checkbox"/>
4.	Do not recommend approval of programme.	<input type="checkbox"/>

Areas for commendation	
1.	Unique programme for which demand was clearly demonstrated in a comprehensive programme document
2.	Programme rationale is clear
3.	Important programme in bridging the gap between technology and management
4.	Impressive alignment to Graduate Attributes at programme level
5.	Exemplary sustainability engagement
6.	Good thought process around adapting cybersecurity modules for this cohort

Conditions of Approval	
1.	Approved modes of delivery should be accurately recorded. The modalities for each module need to be clearly identified.
	Response: All modules will be validated for delivery in two modalities: in-person and online. The Akari system has been updated accordingly to ensure accurate and consistent recording of the approved delivery modes for each module.

Recommendations	
1.	To make explicit in documentation and marketing that this is a conversion programme.
	Response: This has been clearly stated in the programme information section within Akari. We will also ensure that the conversion nature of the programme is explicitly communicated across all marketing materials moving forward.
2.	Provide a programme development plan across all modules to integrate the two aspects of the programme. This cohesion needs to be evident in the programme documentation. What is the plan to integrate/incorporate Cybersecurity context into the Management modules (e.g., case studies)?
	There will be flexibility within certain assessments to tailor them toward a cybersecurity context, particularly within the Leading for High Performance module. Additionally, the Strategic Risk & Crisis Management module will be applied within a cybersecurity framework, as it is not planned to be shared across other disciplines.
	It is also planned that the Project Management module will be delivered with a specific focus on cybersecurity.
	While the remaining management modules may allow for some level of integration with cybersecurity themes, we are more cautious in terms of the extent of alignment that can be guaranteed, as these modules are expected to be shared across programmes.
	The programme team will commit to developing this plan before 2026.
3.	The Programme Development team need to offer a seamless, integrated and cohesive experience for the student, e.g. joint extended induction/orientation; coherence across assessment approaches, schedules and the research project.
	Response: The programme team will develop a plan for an extended and integrated induction/orientation prior to the programme's launch in September 2026. In addition, we are committed to establishing a cohesive assessment strategy that ensures alignment across modules, including assessment approaches, scheduling, and the structure of the research project, to provide a seamless and coherent student experience.
4.	There is a need for regular meetings between the two teaching teams beyond the formal QA-mandated meetings in order to facilitate alignment. Consider proper and balanced representation of the programme team and opportunities for socialisation of staff and sharing of knowledge. This should be addressed before students are recruited.
	Response: The programme is scheduled to commence in September 2026. In advance of this, we are committed to establishing a structured schedule of meetings involving staff from both

	disciplines. These meetings will provide opportunities for socialisation, collaborative planning, and knowledge sharing, beyond the formal QA-mandated engagements. This approach will support alignment across the teaching teams and ensure a cohesive delivery of the programme prior to the recruitment of students.
5.	<p>Consider adding transversal skills to PLOs.</p> <p>Response:</p> <p>Programme Learning Outcome (PLO) 9 has been added to reflect the inclusion of transversal skills:</p> <p>"Apply transferable skills such as teamwork, problem-solving, and communication to manage projects and collaborate effectively across different disciplines."</p> <p>This ensures that key transversal competencies are explicitly addressed within the learning outcomes of the programme.</p>
6.	<p>All free electives must be mapped to PLOs.</p> <p>Response:</p> <p>The free elective has been mapped to Programme Learning Outcome (PLO) 9, which focuses on the application of transferable skills such as teamwork, problem-solving, and communication across diverse project and disciplinary contexts.</p>
7.	<p>Recommend validating modules in at least 2 modalities. Consider the 4 approved modalities for flexibility as supported by QA. If any modules are designed for blended or online delivery, alignment with the QQI Statutory Quality Assurance Guidelines for Blended Learning and Fully Online Learning Programmes is required.</p> <p>Response:</p> <p>All modules have been validated for delivery in both in-person and online modalities to ensure flexibility and accessibility. Where applicable, alignment with the QQI Statutory Quality Assurance Guidelines for Blended Learning and Fully Online Learning Programmes will be maintained to support the quality and integrity of delivery in these modes.</p>
8.	<p>Some of the modules on offer do not fully reflect the stakeholder feedback and therefore the panel strongly recommends that the programme development team reconsider some of the core Management modules on the programme, e.g. Finance for Strategic Decision Making.</p> <p>Response:</p> <p>In response to stakeholder feedback, the programme team has revised the structure by moving the Finance for Strategic Decision Making module to the elective pool. Additionally, new electives focusing on Project Management and Innovation have been introduced to better align with stakeholder needs and expectations.</p>
9.	<p>Given that cybersecurity is a fast-moving landscape, consideration should be given to broadening elective opportunities, particularly in industry, in areas such as Innovation Management; Project Management, and Entrepreneurship.</p> <p>Response:</p> <p>To address the evolving nature of the cybersecurity landscape and in line with the panel's recommendation, the Project Management module (MGMT1054) and the Innovation Management module (INNT1002) have been added to the suite of electives. These additions provide students with broader opportunities to develop industry-relevant skills in areas such as innovation, project delivery, and strategic thinking.</p>

10.	Recommend mapping to SFIA Skills Framework for Information Age for a broader perspective in terms of operations. Consider also how Agile project management methods and project management strategies can enhance cybersecurity (see https://instituteprojectmanagement.com/blog/agile-and-project-management-in-cybersecurity-optimisation/). Case studies are available at the following link: https://www.ponemon.org/research/ponemon-library/ponemon-library.html
	<p>Response: We acknowledge the recommendation to map the programme content to the SFIA (Skills Framework for the Information Age) to provide a broader operational perspective. This will be explored during the curriculum design phase to ensure alignment with industry-recognised competencies and skills frameworks.</p> <p>We also recognise the value of integrating Agile project management methodologies and broader project management strategies to enhance the effectiveness of cybersecurity operations. The resource provided by the Institute of Project Management will be reviewed to identify relevant practices and examples that can inform both the Project Management module and the practical components of the programme.</p> <p>Additionally, the case studies available via the Ponemon Institute will serve as valuable material to support teaching, particularly in illustrating real-world cybersecurity challenges and responses. These resources will be considered for integration into relevant modules to strengthen applied learning and contextual understanding.</p>

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Other matters to be brought to the attention of Faculty Board and/or University Programmes Board

It is noted that these programmes like all others within TU Dublin will need to reflect University assessment regulations including award classifications that are approved for implementation in September 2025.

Section G - Approvals

Validation Report

This report has been agreed by the Validation Panel and is signed on their behalf by the chairperson.

Chairperson: Fiona Murray

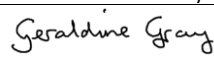
Signed: 

Date: 27/03/2025

School Response

The response to the conditions and recommendations has been agreed by the School and is signed by the Head of School.

Head of School: Geraldine Gray

Signed: 

Date: 28th March '25

Faculty Board

The report and response have been approved by Faculty Board

Vice-Dean for Education:

Signed:	Date: Click or tap to enter a date.
---------	-------------------------------------

University Programmes Board (Programmes of 30 ECTS or great)	
The report and response have been approved by the University Programmes Board	
Registrar:	
Signed:	Date: Click or tap to enter a date.