European Approach for Quality Assurance of Joint Programmes

EVALUATION REPORT

CYBERUS Erasmus Mundus Joint Master in Cybersecurity

Université Bretagne Sud (France)
University of Luxembourg (Luxembourg)
Université Libre de Bruxelles (Belgique)

October 2025

Rapport publié le 26/11/2025

High Council for the evaluation of research and higher education

The consortium of the CYBERUS Erasmus Mundus Joint Master in Cybersecurity has mandated Hcéres to carry out the evaluation of its joint master programme. The evaluation is based on the 'European Approach for Quality Assurance of Joint Programmes', adopted in May 2015 by European Higher Education Area Ministers. These standards are available on the Hcéres website (hceres.fr).

In the name of the expert panel[1]:

Bart PRENEEL, Chair of the panel

In the name of Hcéres[1]:

Coralie CHEVALLIER, President

[1]In accordance with articles R. 114-15 and R. 114-10 of the Research Code, evaluation reports are signed by the chair of the expert panel and countersigned by the President of Hcéres.

CONTENTS

I. STUDY PROGRAMME IDENTITY SHEET

- **Study programme name:** CYBERUS Erasmus Mundus Master in Cybersecurity
- **Speciality:** Cybersecurity
- **Year of creation and context:** The programme started in January 2022 as an Erasmus Mundus Joint Master programme. It is funded until the end of 2027.
- **Partner institutions:**
  - *Université Bretagne Sud* (UBS), France – Coordinator
  - University of Luxembourg (UL), Luxembourg
  - *Université Libre de Bruxelles* (ULB), Belgium
- **Sites where the programme is taught:**
  Year 1:
  - UBS: Lorient, France
  - TalTech: Tallin, Estonia (two-week Winter School)

  Year 2:
  - ULB: Brussels, Belgium (semester 3 for the Internet of Things cybersecurity track students)
  - UL: Luxembourg (semester 3 for the Software cybersecurity track students)
- **Academic degrees awarded:** Double degree between UBS and ULB in the IoT Cybersecurity track and Double degree between UBS and UL in the Software Cybersecurity track. The exact names of the degrees are:
  - UBS: *Master mention Ingénierie des systèmes complexes*
  - UL: Erasmus Mundus Joint Master in Cybersecurity
  - ULB: *Master en Cybersécurité*
- **Regular study period:** 2 years
- **Number of ECTS:** 120 ECTS
- **Tuition fees per year:**
  - For scholarship holders and fee waiver beneficiaries: free
  - For other students: 4,500€
- **Component, faculty or department involved:**
  - UBS: Faculty of Science and Engineering Science
  - UL: Faculty of Science, Technology and Medicine
  - ULB: Brussels School of Engineering and Faculty of Science

METHODS AND RESULTS OF THE PREVIOUS ACCREDITATION(S)

- **No previous evaluation nor accreditation at the level of the joint programme.**

HUMAN AND MATERIAL RESOURCES DEDICATED TO THE PROGRAMME

- **Human resources**

	UBS	UL	ULB
Programme director	1		
Academic coordinators	1	1	1
Administrative staff	3	1	2
Gender advisor	1		
Teaching staff (including PhD students + non university staff)	19	17	5

The management team is made of one programme director (UBS), 3 programme coordinators (UBS, UL and ULB), one gender advisor (UBS) and 6 administrative staff (3 from UBS, 1 from UL and 2 from ULB)

- **Material resources**

Like all students at UBS, UL and ULB, CYBERUS students can enjoy modern facilities and services. These include digital and IT services that facilitate collaboration, such as an eduroam account, a Teams account for videoconferencing and storage, Wi-Fi access and access to onsite and online libraries.

Learning cybersecurity, the students can use commercial and open-source software such as:

- VirtualBox, a general-purpose full virtualisation software application,

- Wireshark, a network protocol analyser,
- Tcpdump, a data-network packet analyser computer programme,
- MySQL, an open-source relational database service,
- PostgreSQL, an open-source object-relational database system,
- AndroZOO, a library of Android applications,

For physical security, they use the following lab equipment:

- ChipWhisperer-Lite boards in kit 1 versions for teaching material security,
- Single-board computers such as Raspberry PIs,
- STM32 ARM Cortex M33 boards,
- FPGA boards.

And they have access to

- Servers,
- The MeluXina, Luxembourg's new supercomputer.

STUDENT POPULATION: EVOLUTION AND TYPOLOGY OVER THE LAST 2/3 YEARS

- 2022-2024 cohort: 23 students – 22 graduated
- 2023-2025 cohort: 28 students – 29 graduated (one student from the 2022-2024 cohort repeated the second year)
- 2024-2026 cohort: 43 students
- 2025-2027 cohort: 34 students

II. VISIT DESCRIPTION

COMPOSITION OF THE EXPERTS PANEL

- **Bart Preneel,** Chair of the panel and academic expert, Full Professor at KU Leuven, Belgium
- **Besma Zeddini,** Academic expert, CY Cergy Paris University
- **Aline Barthelemy,** Global Chief Information Security Officer, Seb Group
- **John Chukwu Ikechukwu,** Student expert, Joint Master of Science in Applied Cyber Security (CyberMACS)

Hcéres was represented by Sophie Guillet, Head of the cooperation unit, European and International Department.

VISIT DESCRIPTION

The online visit, which took place on 15 and 16 September 2025, was a comprehensive two-half-day review that included a series of meetings with various stakeholders involved in CYBERUS.
During visit, the experts met with representatives and coordinators from each university, including academic and administrative staff, quality assurance staff, students and socio-economic partners. Further details of the visit and the outcomes of these meetings can be found in the following section.

VISIT AGENDA

Nearly 40 participants were met during the interviews.

Monday 15 September 2025

Time	Session		Interviewees
9:00 – 10:00	**1**	**Opening session** - Opening by Hcéres representative - Introduction of the chair and of the expert panel - Brief overview of the programme by CYBERUS programme director followed by discussions with the expert panel	- Programme director (UBS) - Programme coordinators (UBS, UL, ULB) - Vice President International (UBS) - Counsellor to Vice President Academic (ULB)
10:00 – 11:00	**2**	**Meeting with the academic staff**	- Associate professor of Software engineering and gender adviser (UBS) - Cybersecurity Innovation Engineer (UBS) - Assistant professor in Software Engineering for AI Systems (UL) - Associate professor for Resilient Cyber-Physical Systems (UL) - Associate professor in Cyber Defence and Distributed Networks (ULB) - Privacy researcher (ULB)
11:00 – 11:15	Health break		
11:15 – 12:00	**3**	**Meeting with the administrative staff**	- Head of the International Office (UBS) - Administrative and Financial Officer (UBS) - Study Programme Administrator (UL) - Research facilitator (UL) - Administrative assistant (ULB)

12:00 – 13:00	**4**	**Meeting with the socio-economic partners and the alumni**	- Alumnus from Nepal, graduated in 2024, Security Research Engineer at NEC Laboratories Europe, Germany - Alumna from Pakistan, graduated in 2024, Doctoral researcher at Interdisciplinary University of Luxembourg Centre for Security, Reliability and Trust (SnT), Security, Reasoning and Validation (SerVal) Group. - Researcher in cybersecurity at Thalès, France. - Embedded Systems Architect at Volvo Construction Equipment, Sweden - Chief Information Officer at Belfius Bank and Insurance, Belgium - Chief Technology Officer at itrust Abstractions Lab, Luxembourg
13:00 – 13:30	**Experts debriefing session**		

Tuesday 16 September 2025

Time	**Session**		**Interviewees**
9:00 – 10:00	**5**	**Meeting with students**	- Egyptian second-year student from UL - German second-year student at UL - Algerian 2025 graduate from UL and UBS - Austrian 2025 graduatefrom UL and UBS - Kenyan second-year student from ULB - Moroccan second-year students from ULB - French 2025 graduate from ULB and UBS - Nigerian 2025 graduate from ULB and UBS
10:00 – 11:00	**6**	**Meeting with the quality assurance staff**	Head of Careers Office (UBS) - Quality Assurance Department (ULB) - Strategic Projects Department (ULB) - Project Manager, Faculty of Science, Technology and Medicine (UL)
11:00 – 11:15	Health break		
11:15 – 11:45	Experts debriefing session and preparation for session 7		
11:45- 12:45	**7**	**Closing dialogue**	- Programme director (UBS) - Programme coordinators (UBS, ULB)
12 :45- 13 :15	Expert debriefing session		

III. EVALUATION REPORT

1. ELIGIBILITY

Level of compliance		
Compliant	Compliant with conditions	Non-compliant

1.1 STATUS

The Erasmus Mundus CYBERUS programme is delivered by three universities: UBS (*Université de Bretagne Sud*), UL (University of Luxembourg) and ULB (*Université Libre de Bruxelles*). At the time of the programme's inception, UBS had already seven cybersecurity degrees, meaning they had the necessary resources and expertise. The French region of Brittany is also very active in the field of cybersecurity with initiatives such as the 'Bretagne Cyber Campus'. ULB already offered a joint master's degree in cybersecurity and systems design and analysis with other Belgian institutions and it has founded a cybersecurity research centre focusing on securing the Internet of Things (IoT) in 2017. UL had extensive experience in software cybersecurity research, but prior to CYBERUS it did not offer a master's degree in cybersecurity. Recently, UL has started a new master's programme in cybersecurity and cyber defence. It is also worth noting that the three universities were collaborating on research prior to this programme. All three universities are fully recognised in their respective countries.

Therefore, the three universities have the relevant expertise and proper accreditations to support the programme.

The programme focuses on cybersecurity in computing, with 105 out of 120 credits dedicated to this area. After the first year at UBS, which covers the fundamentals of cybersecurity, students can choose between two specialisations.

- IoT Cybersecurity, delivered by ULB;
- Software Security, delivered by UL.

In addition, a Winter School is organised in Estonia, home to the NATO Cooperative Cyber Defence Centre of Excellence. The spring School provides students with the opportunity to meet alumni, take part in a *Capture The Flag* (CTF) cybersecurity competition, and attend presentations delivered by guest researchers distinct from their regular lecturers.

The main objective of the programme is to train cybersecurity experts at master's level, offering a balanced combination of academic knowledge and practical experience. This practical dimension is achieved through two internships: one of 5 ECTS in the first year and another 30 ECTS in the second year. Students are also made aware of diversity issues through exposure to different cultures, languages, and academic environments. Upon completion of the programme, graduates are expected to be fully prepared to enter the job market or to pursue doctoral studies. The entire master's degree is taught in English

For now, a joint degree is not issued under CYBERUS due to constraints imposed by national legislations. Instead, students receive double degrees as follows:

- From UBS and ULB for the *IoT Cybersecurity* track;
- From UBS and UL for the *Software Cybersecurity* track.

1.2 JOINT DESIGN AND DELIVERY

The master's programme has been jointly designed by the three universities. The existing collaboration among them provided an ideal environment for the inception and design of the programme, enabling each university to contribute its specific expertise to support the master's degree and its specialisation tracks.

Responsibilities are distributed as follows:

- Université Bretagne Sud (UBS) is responsible for coordinating the three universities, delivering the first-year teaching, organising the Winter and Spring Schools, and overseeing the first-year internship;
- Université Libre de Bruxelles (ULB) is responsible for teaching the *IoT Cybersecurity* track in the second year;
- University of Luxembourg (UL) is responsible for teaching of the *Software Cybersecurity* track in the second year;
- All three universities share responsibility for supervising the second-year internship; for administrative and practical reasons, the internship agreement is signed between the hosting company and either ULB or UL.

UBS has assumed a broader range of responsibilities, reflecting its greater availability of resources to support these tasks.

While teaching is conducted in English, collaboration between the three universities is mainly carried out in French, facilitating communication among academic and administrative teams.

The grading methodology has been harmonised across the three universities to ensure consistent grading standards.

Although it was initially planned that the end-of-semester examination commission would bring together representatives from three universities, this proved challenging due to differences in academic calendars. However, the final examination commission is systematically convened with representatives from each of the three universities.

1.3 COOPERATION AGREEMENT

The three universities have set up and signed an extensive cooperation agreement knows as the 'Consortium Agreement'.

The agreement covers the following key elements:

- Denomination of the degrees awarded in the programme, 'CYBERUS Erasmus Mundus Joint Master in cybersecurity', as per Consortium agreement Section 8.1;
- Coordination and responsibilities of the partners involved in management and financial organisation, including funding, costs and income sharing, etc. The roles and duties of the partners are described in Section 5, the governing bodies in Section 6 and the financial management in Section 7. Regarding the governing bodies, it was indicated that the members of these bodies frequently overlap. At the next revision of the consortium agreement, it may be sensible to simplify the governing bodies;
- Admission and selection procedures for students are covered in Section 11.
- As regards the mobility of students and teachers, only the former is addressed in Section 8.5.
- Examination regulations, student assessment methods, recognition of credits and degree awarding procedures in the consortium are covered in Section 8.

The expert panel noted that the student eligibility process changed significantly between 2023 and 2024, leading to a sharp increase in the eligibility rate—from 25% to 95%. This rise can be explained by a procedural adjustment that allowed part of the required documentation to be submitted after students had been selected, thereby simplifying the application process and making it easier for candidates to qualify.

The self-evaluation report highlights that the management structure outlined in the Consortium Agreement is likely too complex. The General Management Board, composed of representatives from the senior management of the three universities, has never convened. The Project Steering Board and the Integrated Faculty Board have been merged, with most summer meetings held in person and winter meetings conducted online. At the time of the visit, the International Advisory Board, which was expected to review the programme surveys, had not yet been established. With regard to quality assurance, although an external evaluation by an

EQAR-registered agency was initiated—namely this evaluation—no 'Internal and External Evaluation Operational Committee' has yet been established. This aspect will be further detailed in *Standard* 9.

From the interviews, the expert panel concluded that the master's programme is efficiently managed from an operational perspective, with effective communication and the emergence of a shared institutional culture among the partners. However, governance could be further strengthened by devoting greater attention to strategic coordination and by deepening the integration of quality assurance.

2. LEARNING OUTCOMES

Level of compliance		
Compliant	Compliant with conditions	Non-compliant

2.1 LEVEL [ESG 1.2]

Sixteen learning outcomes have been defined that cover cybersecurity in a comprehensive manner. Five are mainly acquired at university, seven are acquired both at work and at university, and four are mainly acquired in a professional environment.

The five university-based learning outcomes are technical in nature and supported by the combined expertise of the three partner universities:

- Design and develop secure products and security architectures;
- Test the resistance of software, products and embedded systems to the latest cyber threats;
- Determine and analyse product vulnerabilities and security solutions, and take appropriate countermeasures to reduce the risk of exploitation;
- Monitor cyber threat and cybersecurity developments;
- Develop original research.

The seven learning outcomes acquired both at university and in the workplace focus on methodological, professional, and interpersonal skills:

- Apply an interdisciplinary approach to cybersecurity;
- Use professional knowledge and skills;
- Work responsibly and ethically as individuals and as team members or leaders;
- Apply essential concepts, principles, and practices, showing judgment in the selection and application of technologies and methods in research and development;
- Measure the performance and troubleshoot cybersecurity systems, Implement cybersecurity solutions and practices, information assurance, and cyber/computer forensics software/tools;
- Operate in unison within EU cyber strategy and policies and advise top management;
- Work smoothly and operate fluently in a multicultural environment.

The four learning outcomes acquired in the workplace are essential for professional practice in the cybersecurity sector:

- Manage and transform complex, sometimes unpredictable, environments that require new approaches;
- Identify, analyse, and evaluate the cybersecurity needs of an organisation;

- Design operational and strategic cybersecurity strategies and policies;
- Progress to managerial, consultancy, or research positions after a few years' experience.

Based on the syllabi reviewed, the panel concludes that the level of the learning outcomes is appropriate for a master's programme, preparing students to operate effectively in complex and unpredictable professional contexts. The outcomes correspond to the Framework for Qualifications in the European Higher Education Area as well as to the respective national qualification frameworks. The emphasis on research ensures that graduates are capable of conducting high-level research in cybersecurity.

The panel recommends rephrasing the final learning outcome to indicate that the programme is 'laying the foundations' for such professional advancement, thereby making it more directly applicable to students upon graduation. This also implies that the second-year internship should maintain sufficient relevance to students' future professional environments.

In view of the rapid progress in the development of generative AI and its significant impact on the cybersecurity sector, the panel recommends revising the learning outcomes to ensure that the programme reflects these technological and methodological advances.

Overall, the panel concludes that the programme's learning outcomes are fully consistent with the level expected within the Framework for Qualifications in the European Higher Education Area (FQ-EHEA). Nonetheless, one outcome should be reformulated, and the overall set of learning outcomes should be reviewed in light of emerging developments in generative AI.

2.2 DISCIPLINARY FIELD

The programme offers a coherent set of learning outcomes, equipping students with the technical expertise, knowledge, and competencies required for a professional career in cybersecurity.

This master's programme focuses developing advanced technical proficiency in computer science. It covers four core computing disciplines: information technology (for all students), computer science and computer engineering (for students enrolled in the IoT Cybersecurity track) and software engineering (for students in the *Software Cybersecurity* track). Upon reviewing the syllabi, the expert panel has noted that some domains, such as network security, would benefit from more comprehensive coverage during the first year.

The programme also addresses the interdisciplinary and governance dimensions of cybersecurity, such as risk management and regulation, which are essentially for enabling students to progress beyond purely technical roles. However, the relationship between cybersecurity and other interdisciplinary subjects such as geopolitics, criminology, psychology and economics could be made explicit.

The programme would further benefit from being aligned with recognised international cybersecurity education frameworks, such as the: ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guidelines (https://cybered.acm.org/); UK Cybok (https://www.cybok.org/); ENISA Cybersecurity Skills Framework (https://enisaeu.github.io/ECSF/).

The panel concludes that the programme's learning outcomes are appropriate for the field of cybersecurity. However, it recommends expanding on the interdisciplinary aspects and explicitly positioning the programme within these international educational frameworks.

2.3 ACHIEVEMENT [ESG 1.2]

The panel analysed the course syllabuses, reviewed internship and master's thesis topics, and discussed their content during interviews with students, alumni, and supervisors. While the syllabi clearly set out the intended learning outcomes, the mapping between these outcomes and the corresponding assessment methods could be documented more systematically.

The academic learning outcomes demonstrate appropriate technical depth and complexity. However, some students reported difficulties in applying their knowledge in practical settings—particularly during *Capture the Flag* (CTF) competitions. Students without a solid computer science background also face additional

challenges, which could be addressed either through stricter admission criteria or through targeted preparatory courses in the first year to bridge technical gaps.

During interviews with alumni supervisors of master's theses in industry, and current students, overall feedback was very positive. Most graduates have secured employment in the cybersecurity sector or progressed to research positions. Some alumni, however, mentioned that certain cybersecurity roles within the EU require EU citizenship which can be a barrier to employment. The CYBERUS programme coordinators are aware of this constraint.

The relevance of the Year 2 internship is critical to achieving several intended learning outcomes, such as 'identify, analyse and evaluate the cybersecurity needs of an organisation' and 'design operational and strategic cybersecurity strategies and policies'. The panel has noted that many students undertake their second-year internships in research laboratories, where it may be challenging to meet these outcomes Fully. The panel therefore recommends that the programme coordinators ensure that such internships remain adequately aligned with professional objectives.

Besides, the programme currently offers no formal support for students wishing to obtain professional cybersecurity certifications, such as CISSP and CISM, which are highly valued by employers. The panel recommends that the programme provides advice or opportunities for students seeking to pursue such certifications during their studies.

While the three universities collaborate with industry and several lecturers are active professionals, the number of formal partnerships with cybersecurity organisations ('Associated Partners' as referred to in Section 7.1 of the Consortium Agreement) remains limited. This may restrict students' exposure to practical training with key cybersecurity tools, particularly for those completing internships in research environments. The panel recommends expanding formal partnerships to give students broader access to state-of-the art commercial tools used in the field.

Overall, the panel concludes that the programme successfully achieves the intended learning outcomes and that graduates are well prepared for employment in industry or for doctoral research. The panel encourages the programme to provide structured support for obtaining professional certifications.

2.4 REGULATED PROFESSIONS

Not applicable for the CYBERUS programme.

3. STUDY PROGRAMME [ESG 1.2]

Level of compliance		
Compliant	Compliant with conditions	Non-compliant

3.1 CURRICULUM

The CYBERUS Joint Master is a two-year programme (120 ECTS) delivered jointly by the consortium partners. It is structured over four semesters and designed to balance advanced technical expertise in cybersecurity with transversal skills such as entrepreneurship, innovation, and research training.

- Semester 1 (30 ECTS) establishes a common foundation, including through compulsory courses such as *Secure Advanced Programming* and *Entrepreneurship*. These modules aim to harmonise the diverse academic backgrounds of incoming students and provide solid bases in secure coding, information security, and innovation principles.
- Semester 2 (30 ECTS) builds on this foundation by introducing advanced modules such, operating system security, and secure networking. The focus is on technical mastery and professional skills achieved through hands-on laboratories and project-based learning.

- Semester 3 (30 ECTS) allows for specialisation and flexibility. Students can select electives such as digital forensics, penetration testing, or governance and risk management, as well as pursuing an entrepreneurship project. At this stage, students also begin to define their thesis or internship project.
- Semester 4 (30 ECTS) is entirely dedicated to a thesis or professional internship conducted within a consortium partner laboratory or industry. This ensures alignment between academic learning and professional practice.

Mobility is embedded within the programme design: students must study at least in two of the consortium institutions and participate in a Winter School in Tallinn, Estonia. This mobility component exposes students to diverse academic, cultural, and institutional contexts, enriching both their academic and personal experience.

The curriculum is clearly structured and effectively supports the achievement of the intended learning outcomes. It strikes a balance between academic rigour and practical training, while integrating transversal competencies that foster broader professional and personal development. The joint European delivery of the programme further strengthens its international and intercultural dimension.

The curriculum demonstrates a coherent progression from foundational knowledge to advanced specialisation and professional application. The first year focuses on fundamentals and advanced technical courses, while the second year offers opportunities for specialisation and applied learning. Integrating entrepreneurship across multiple semesters reinforces innovation capacity ensures that students are exposed to both technical and managerial perspectives. The close linkage between coursework and the final thesis or internship consolidates learning and bridges academic and professional practice.

However, several areas could be further developed. The workload may be perceived as demanding due to the combination of advanced technical courses and transversal modules. The network security component in Year 1 could be strengthened, as the *Operating Systems Security and Networking* course appears to focus primarily on operating systems. Students enrolled in the *IoT cybersecurity* track seem to gain limited exposure to topics such as cloud computing, artificial intelligence, blockchain, and distributed ledgers. The title of *INFO-F-537 Cryptanalysis*" should be revised to better reflect its actual content. In addition, some overlaps exist between the entrepreneurship course in Year 1 and the elective on entrepreneurship at ULB in Year 2. Finally, clearer guidance linking the Semester 3 electives to the thesis or internship would strengthen programme coherence and student navigation.

In conclusion, the CYBERUS Master's degree is a well-structured and balanced two-year programme (120 ECTS) that brings a natural progression from fundamentals to applied practice. Students benefit from an extensive mobility component across the three partner institutions. The panel suggests updating and streamlining certain elements of the curriculum.

3.2 CREDITS

The programme consistently applies the European Credit Transfer and Accumulation System (ECTS). Each semester corresponds to 30 ECTS, amounting to a total of 120 ECTS upon completion. The allocation of credits is documented in the syllabi and reflects the expected workload of lectures, laboratory sessions, project work, and the thesis or internship.

The credit distribution is transparent and consistent with standards for joint master's programmes corresponding to the second cycle of the Framework for Qualifications in the European Higher Education Area. Each semester contributes equally (30 ECTS), while the final thesis or internship, weighted at 30 ECTS, appropriately reflects its significance within the programme.

3.3 WORKLOAD

The CYBERUS joint master amounts to 120 ECTS over two years, consistent with the expected workload for a second-cycle degree within the European Higher Education Area. Programme documentation confirms that one ECTS credit corresponds to approximately 25–30 hours of student work, encompassing lectures, laboratory sessions, project work, and independent study.

The overall workload thus aligns with European norms (90–120 ECTS for a master's degree). The balance between coursework (90 ECTS) and the final thesis or internship (30 ECTS) is appropriate. While some feedback from the online visit indicated that the workload can be demanding, the academic and administrative support provided ensures that completion within the two-year timeframe remains feasible. All students managed to graduate on time; except for one who had difficulties finding an internship and had to repeat the second year. Processes for monitoring workload, such as student feedback and regular review by the joint programme's governance bodies, are in place.

4. ADMISSION AND RECOGNITION [ESG 1.4]

Level of compliance		
Compliant	Compliant with conditions	Non-compliant

4.1. ADMISSION

The CYBERUS joint master's programme has established a clear, transparent, and standardised admissions process applied across the consortium. It targets students holding a Bachelor's degree (minimum 180 ECTS) in computer science, information technology, electrical engineering, or a related discipline, ensuring that candidates possess the necessary academic background for advanced studies in cybersecurity.

The selection procedure is conducted annually through a joint online application system coordinated by the consortium. The process includes:

- submission of academic transcripts and degree certificates;
- proof of English language proficiency (minimum B2/C1 level, as the programme is delivered entirely in English);
- letters of motivation and recommendation;
- a CV highlighting academic and, if applicable, professional experience.

Applications are first checked for eligibility and subsequently assessed by an Admissions Committee composed of representatives from the partner institutions. Evaluation Criteria include academic performance, relevant disciplinary knowledge, motivation to pursue a career in cybersecurity, and potential for success in an international joint master's environment.

The programme ensures transparent and accessible communication with prospective applicants. Information regarding entry requirements, deadlines, and selection criteria is clearly available on the consortium's website and online application portal.

The admission requirements are appropriate for the level and discipline of the programme, ensuring that only students with the necessary technical competence and English proficiency are admitted. The use of a joint selection committee guarantees fairness and transparency, while the online application platform facilitates accessibility for international candidates.

The expert panel commends the following strengths of the admission procedure:

- clear academic entry requirements aligned with programme's demands;
- transparent and standardised procedures across all consortium partners;
- multistage evaluation process combining eligibility check and selection by committee;
- strong international accessibility through a digital application system and open communication;
- excellent gender balance (close to 50/50, compared to the typical 75/25 in cybersecurity).

However, the panel identified a few challenges and potential areas for improvement. These include the limited recognition of non-traditional backgrounds, such as applicants from interdisciplinary fields or professional with practical experience in cybersecurity but without a formal computing degree. Furthermore, the consortium's diversity and inclusion strategies could be developed further to promote broader academic diversity, for example by welcoming applicants with interdisciplinary or professional backgrounds. Continued attention should also be given to the inclusion of students from varied socioeconomic backgrounds, while maintaining the programme's excellent gender balance.

Overall, the panel concludes that the admission requirements are well aligned with the level and discipline of the programme. The admissions process is carefully designed and effectively implemented to attract high-potential students from diverse backgrounds while maintaining an exemplary gender balance. The panel encourages further attention to applicants from non-traditional backgrounds and underrepresented populations.

4.2. RECOGNITION

Mobility between consortium partners is fully recognised. All courses and credits completed at one partner institution are automatically validated and transferred through the use of ECTS and the Diploma Supplement systems. The Consortium Agreement guarantees mutual recognition of learning outcomes, assessment methods, and academic credits.

Recognition of prior learning (RPL) is possible in specific circumstances, based on documented professional experience or previous studies, provided that equivalence with the programme's intended learning outcomes can be demonstrated.

Overall, the panel concludes that the recognition procedures are consistent with European standards and ensure seamless mobility across partner institutions. The use of ECTS and harmonised learning outcomes facilitates academic recognition and transparency. Although recognition of prior experiential learning is not yet highly developed, this does not impede student progression, as the programme primarily targets recent bachelor's degree graduates.

5. LEARNING, TEACHING AND ASSESSMENT [ESG 1.3]

Level of compliance		
Compliant	**Compliant with conditions**	Non-compliant

5.1 LEARNING AND TEACHING

The programme is clearly structured and well organised, offering a wide range of learning activities. It combines regular lectures with hands-on exercises and laboratory sessions. Projects are completed either individually or in groups, with group composition designed to ensure diversity of academic and cultural background. Students participate in an international *Capture The Flag* (CTF) exercise, a gamified approach to penetration testing. During the internship and master's thesis, the focus shifts to conducting an individual research project in either an industrial or academic environment. The academic staff collectively possess the expertise required to deliver the intended learning outcomes. In the first year, approximately 40% of teaching is delivered by academics from other universities and by industry professionals, thereby adding significant expertise to the programme.

The programme is well-balanced and aligned with its learning outcomes. However, the panels notes that the common component shared by both specialisation tracks (IoT and Software Security) could be expanded. In particular, all students should gain sufficient knowledge in incident management, network security, artificial intelligence, cloud security, blockchain, and distributed ledgers. Currently, some of these topics are covered only within one of the tracks. Students undertaking their master's thesis in a university laboratory or performing highly technical work in industry could benefit from greater exposure to governance and policy dimensions of cybersecurity. This could be achieved by integrating a specific assignment within the internship or by requiring students to reflect on the broader societal or regulatory implications of their research. At ULB, sessions on

research methodology in preparation for the master's thesis are currently optional; the panel recommends making these sessions mandatory.

Each partner university operates its own internal quality assurance processes to monitor the quality of courses and programme delivery. A committee reviews student feedback and communicates findings to the relevant academic staff. The panel's review of evaluation results and discussions with students indicate that satisfaction levels are high. While some students reported logistical issues (e.g., with remote lectures) and occasional overlap between some courses, the programme management has taken appropriate corrective measures. As Erasmus Mundus students spend only one year at each university, it is understandably difficult to involve them directly in the committees discussing feedback from course evaluations. The panel notes that while there is an adequate process for communicating issues to the programme director, a coordinated quality review process has not yet been established at the level of the joint programme. Coordination between courses currently occurs an ad hoc basis (for example, in cryptography) and should be further formalised (see *Standard* 9).

The first-year curriculum is fixed, except for language courses, which may vary depending on prior knowledge. Students lacking background in specific technical areas are encouraged to bridge these gaps through self-study. The internship topic provides scope for pursuing individual interests. In the second year, students select one of two optional courses. with further electives available in the UL and ULB syllabi. The panel observed some overlap between the entrepreneurship courses offered in the first and second years. The 30-ECTS master's thesis offers a valuable opportunity for students to expand their expertise in area chosen field. The programme has also shown flexibility in accommodating students facing personal difficulties.

The panel notes that peer-to-peer learning has not been explored beyond group projects, which already brings together students from diverse backgrounds. As the first cohort of alumni enters the labour market, the panel recommends developing alumni engagement mechanisms, such as mentorship opportunities or guest lectures.

The management team is well prepared to support students with special needs, although, demand for this support has so far been minimal. Students who need such support are referred to the local support services at each partner universities. This enables them to receive special adjustments for the courses. Students facing personal issues or health-related issues are offered sufficient flexibility to continue their studies.

Overall, the panel concludes that the curriculum is well balanced, and aligned with the intended learning outcomes. The panel recommends exploring peer-to-peer learning opportunities and establishing collaborations with the growing number of alumni.

5.2 ASSESSMENT OF STUDENTS

According to the self-evaluation report, the programme employs a broad range of assessment methods, including oral examinations, written tests, individual and group presentations, and evaluations of classroom participation. These assessments are implemented in accordance with the regulations of each partner university.

In cases of failure, students are permitted one resit examination. If a student fails to complete a semester, they must repeat it as self-funded student. Such cases remain rare, reflecting the competitive admissions process and the close academic supervision provided.

During interviews, students expressed satisfaction with the overall assessment system. However, some noted that assessment criteria or rubrics were not always provided at the start of courses and that more detailed criteria would have been helpful. They also requested more detailed feedback on assignments and presentations would be helpful. The panel therefore recommends that the consortium standardise and document the feedback process across all courses to support student learning and progression.

The assessment of the master's thesis at ULB and UL follows local procedures, which include an oral defence before at least two examiners. While a ULB staff member may be invited to participate remotely, there is no formal requirement to ensure representation from at least two universities.

No consortium-wide review has yet been undertaken to analyse assessment methods and map them systematically against learning outcomes across all courses. The panel encourages the consortium to conduct such a mapping exercise, which would also strengthen coordination of assessments between the universities.

Feedback from thesis supervisors and alumni indicates that graduates are well prepared for employment, and that a substantial number of students continue to doctoral studies, reflecting the strong academic level achieved.

The programme management and teaching staff are aware of the implications of generative AI for assessments. They have already adapted by placing greater emphasis on oral presentations and interactive evaluation formats. Broader institutional policies are being developed within each university. The panel recommends continuing to monitor developments in generative AI to ensure that assessments remain valid and that learning outcomes evolve to include competencies in the responsible use of AI tools for cybersecurity practice.

Students with special needs or specific circumstances receive appropriate adjustments for assessment process (e.g. extended time or rescheduled examinations).

Overall, the assessment of students is working well but could be improved to fully meet the expectation of the standard. A broad range of assessment methods is in use, and the quality of master's thesis demonstrates that students are well prepared for professional and academic careers. Nevertheless, the panel recommends the following improvements: creating a formal mapping between course assessments and learning outcomes; ensure that faculty members from at least two universities participate in all master's thesis defences; expand and standardise the feedback provided to students; maintain vigilance regarding the impact of generative AI on assessment validity.

6. STUDENT SUPPORT [ESG 1.6]

Level of compliance		
Compliant	Compliant with conditions	Non-compliant

The CYBERUS programme' student support service is a comprehensive system that successfully identifies and addresses the challenges faced by its students. Support begins at the point of admission and continues throughout the entire duration of the programme. It includes guidance on visa and residence permits, assistance with accommodation and administrative procedures, support in securing suitable internships, and continuous academic, health, and personal support, extending to thesis and preparation for graduation. Interviews with students, alumni, and employers, as well as the Self-Evaluation Report, provide evidence that the programme offers strong and responsive support in multiple areas.

Each partner university employs dedicated administrative staff who act as primary contact points, ensuring smooth communication between students, teaching staff, and programme directors. These staff members assist with all aspects of student life, from registration to the resolution of day-to-day administrative issues. Given that students study across three universities – UBS, ULB, and UL – and navigate different national administrative systems, visa and residency procedures represent one of the most significant challenges, particularly for non-EU students. The process of converting mobility visas into residence permits upon arrival can be lengthy and stressful. However, the programme's administrative staff are proactive in liaising with ministries and immigration authorities on students' behalf. Although visa and residence permit issues remain systemic challenges, the responsiveness and commitment of the staff significantly mitigate their impact and reassure students of the consortium's dedication to their well-being.

During the first two weeks of Year 1, a detailed welcome programme is organised to address all administrative and logistical matters and to facilitate team building; the number of lectures during this period is deliberately limited. In Year 2, students are invited to participate in their host university's welcome week, which includes a specific session dedicated to the CYBERUS programme.

Internships play a pivotal role in the CYBERUS learning experience and are closely linked to the programme's employability outcomes. Despite the inherent complexities of securing placements, the consortium actively engages employers and partners early in the academic year to ensure that opportunities are finalised in good time. Students are also free to seek their own placements, provided that these align with programme objectives. Internship supervisors confirmed that students consistently meet expectations, particularly in terms of technical

preparation, and integrate smoothly into workplace environments. Graduates reported that their internships experiences enhanced their professional readiness and influenced their career paths. These findings confirm that the internship framework makes a valuable contribution to employability and creates a meaningful bridge between academic study and professional practice.

The programme also places strong emphasis on well-being and inclusion. Each partner university offers confidential medical and psychological support services, which students can access independently. Support for students with disabilities includes additional examination time, physical accessibility measures, and financial assistance for external support when required. These provisions ensure that students with specific needs receive appropriate support from admission to graduation. The small size of the programme community also allows for flexibility in individual cases, such as pregnancy, hospitalisation, or other personal difficulties, ensuring that no student is left behind.

Financial support is another strength of the programme. Scholarship holders receive monthly Erasmus Mundus stipends, and all students benefit from accommodation funded by the consortium for the winter schools. In cases of financial hardship, the consortium has also covered transportation costs to enable students' participation in the Winter School. These measures promote equal access to extracurricular opportunities and strengthen fairness and cohesion within the student body.

Overall, the student support services are comprehensive, well-integrated, and clearly contribute to achieving the intended learning outcomes. By addressing mobility-related challenges, supporting employability through internships, and promoting inclusion, well-being, and equity, the programme ensures that students are well supported in achieving both academic and professional success.

7. RESSOURCES [ESG 1.5 & 1.6]

Level of compliance		
Compliant	Compliant with conditions	Non-compliant

7.1 STAFF

The programme is taught by a competent and experienced academic team with extensive international expertise. According to the information provided, UBS employs twenty-four teaching staff members, UL ten, and ULB eight. The team has a strong international profile and is supplemented by additional lecturers during the Summer and Winter schools. In the first year, 40% of courses are delivered by external lecturers, many of whom have substantial industrial experience. The second year also benefits from guest lecturers, albeit to a lesser extent. ULB staff members provide the necessary expertise for the *IoT Cybersecurity* track, while UL staff members specialise in *Software Cybersecurity*. Collectively, they form a strong and well-balanced team, capable of delivering the full scope of the programme.

During the interviews, the panel noted that the academic staff are enthusiastic, highly motivated, and satisfied with their workload. Although some overlaps between courses remain, staff from the different universities communicate informally to coordinate their teaching. Students spoke very positively about the accessibility and responsiveness of their lecturers.

A capable management team has been established to oversee the programme. It is led by an experienced Programme Director, and each institution has appointed an Academic Coordinator. Adequate administrative support is in place, and UBS also designated a Gender Advisor. The programme budget, including Erasmus Mundus funding, is well managed. However, the management structure described in the Consortium Agreement has not been fully implemented with some boards not convening during the first three years. As noted under Standard 1, membership of several governance bodies overlaps, which has reduced the need for formal meetings. Overall, internal communication is smooth and effective, though the panel recommends that communication processes be further formalised to improve consistency.

Although the cybersecurity field is struggling to educate female experts, the CYBERUS programme has made

efforts to achieve an excellent gender balance among its student population, which is promising for the future of the discipline. Among teaching staff, the gender balance is good at UBS but remains limited at ULB, where improvement is still needed.

The panel recommends expanding the training of external lecturers from industry to ensure alignment with academic expectations. Coordination between lecturers teaching the same course and across related courses could also be strengthened. While current mechanisms function satisfactorily, introducing more formal structures for coordination and review would ensure that issues are identified and resolved more systematically.

The Consortium Agreement provides for a network of associated partners, defined as institutions and companies that 'contribute to the implementation of specific tasks and activities' without being full beneficiaries. However, the status of these partners has not yet been formalised. There already exists an informal network of universities and companies as guest lecturers, internship providers, and thesis supervisors, and the participating universities collaborate with industry partners in research projects. Formalising and expanding these collaborations would make them more strategic and sustainable, and could facilitate students access to key industrial cybersecurity tools. The Consortium Agreement also provides the representation of the associated partners on several management boards. The panel considers that including industry and academic experts as board members would be valuable in providing direct feedback on current professional developments and contributing to the ongoing evolution of the programme.

Overall, the panel concludes that the teaching and management staff are highly qualified, motivated, and effective. However, the management structure described in the Consortium Agreement has not been fully implemented. Internal communication operates efficiently but would benefit from further formalisation. The panel recommends expanding collaborations with the associated partners and improving the training of external lecturers.

7.2 FACILITIES

The three participating universities possess the necessary infrastructure to deliver the courses and laboratory work and to support group projects, as well as to host internships and the master's thesis. Each institution provides access to robust hardware and software resources suitable for computer science and cybersecurity courses. Dedicated setups are available for embedded systems security and students can access to high-performance computing resources (e.g., the *MeluXina supercomputer* in Luxembourg) when required for research purposes. Logistical issues concerning facilities are rare and, when they arise, are resolved promptly.

However, the panel notes that students would benefit from broader access to key cybersecurity tools commonly used in industry. The programme already collaborates with several companies willing to provide access to such tools, and the panel encourages the consortium to further expand these partnerships to enhance student's hands on experience.
Overall, the panel concludes that the facilities and services provided are sufficient and of good quality to support the programme's learning activities. It nevertheless recommends exploring additional opportunities to provide students with direct access to the principal cybersecurity tools currently used in industry.

8. TRANSPARENCY AND DOCUMENTATION [ESG 1.8]

Level of compliance		
Compliant	Compliant with conditions	Non-compliant

The programme's website contains comprehensive and publicly accessible information regarding admission requirements and procedures. Its inclusion in the Campus France catalogue of English-taught programmes, has significantly increased visibility, enhanced openness, and helped to attract a larger pool of qualified applicants, thereby strengthening the programme's reputation. Prospective students can easily access all necessary information to prepare a complete application, including details of required English language test scores and the expected academic background.

The scale and outcomes of the admissions process demonstrate its effectiveness. To date, the programme has received 5,480 applications, conducted 427 interviews, registered 128 students, and graduated 51. Among the registered students, 88 received full scholarships, 38 benefited from tuition fee waivers, and two were self-funded. Gender representation is particularly balanced, with 67 male and 59 female students, an impressive achievement in the traditionally male-dominated field of cybersecurity.

The selection process is rigorous and transparent. Applications are first verified for completeness and authenticity, then evaluated according to academic achievement and professional merit. To ensure fairness, candidates are assessed within their national cohort, and the highest-ranked applicants are invited for interviews and further evaluation. Final admission lists are supplemented by waiting lists, enabling highly ranked candidates to replace those who withdraw. This system ensures both equity and consistency in selecting the most qualified applicants.

Each admitted student signs a student agreement with the consortium, detailing the academic framework, financial and administrative procedures, available services, and appeal and complaint processes. This formalised procedure ensures that students fully understand the expectations and regulations governing their studies.

The full curriculum structure is publicly available online, while detailed course content is shared internally with enrolled students rather than published on the website. While this approach limits external visibility, it does not prevent students from accessing the necessary information once enrolled. Moreover, the programme actively incorporates student evaluations at the end of each module to inform curricular updates, helping to maintain relevance and alignment with student experience. While the panel found that information is generally detailed and well maintained, it noted that in some cases, course titles and content were not fully aligned, and that certain syllabi require updating to ensure clarity and consistency.

The examination regulations reflect the diversity of the national systems represented by the three partner universities. Assessment methods include written and oral examinations, project reports, and take-home assignments. Attendance may also contribute to the final grade. Written examinations generally carry the most weight, but all components are factored into the final assessment. Despite these national variations, the consortium provides adequate guidance and coordination to help students navigate the examination requirements without undue difficulty. The panel found that, for most courses, information about assessment methods was clear and communicated in a timely manner. However, in a few instances, details of assignments and grading rubrics were shared late, and some students expressed a desire for more detailed feedback, particularly feedback on specific components of the course.

Overall, the programme demonstrates a high level of transparency and thorough documentation in relation to the admissions, curriculum, assessment, and quality assurance processes. While some areas require improvements, such as the lack of detailed course content on the public website and inconsistent assessment practices between institutions, these shortcomings are acknowledged and addressed through the student agreement, student support mechanisms, structured orientation sessions, and ongoing coordination among partner universities. These measures ensure that transparency is maintained and that students are well informed and supported throughout their studies.

9. QUALITY ASSURANCE [ESG 1.1 & PART 1]

Level of compliance		
Compliant	**Compliant with conditions**	Non-compliant

The consortium has established a comprehensive quality assurance programme framework designed to identify its strengths and weaknesses and to support continuous improvement. In November, first-year students receive a questionnaire from the Programme office addressing logistical and integration issues. Each of the three participating universities conduct online surveys at the end of each course. At UBS, a additional semester feedback meeting with students is organised. Furthermore, surveys of alumni and external experts were

conducted in spring 2025. Any logistical challenges identified by students are addressed using the feedback provided by the programme office.

The online student surveys represent a valuable tool for improving the programme. However, one persistent challenge is achieving a sufficiently high response rate. At UBS, the participation response rate appears adequate, while at UL it remains limited (only 15 to 30 questionnaires were completed for all Year 2 courses, even accounting for the smaller student cohort). In addition to these online surveys, UBS organises in-person feedback sessions which facilitate an open dialogue between students and staff.

UBS provided detailed course-level feedback, which were highly positive. UL submitted only aggregate feedback covering all year 2 courses for the past two academic years. While the students' feedback is generally positive, no results for individual courses or free-text feedback have been made available, making it difficult to draw detailed conclusions. ULB provided high-level statistics covering all master's programmes in Year 2 over the past three years; these data sets do not permit any meaningful conclusions about the specific IoT Cybersecurity track.

Until now, the consortium has largely delegated course-level quality assurance to the participating universities. The panel recognises that it is difficult to actively involve students in committees reviewing feedback, as Erasmus Mundus students spend only one year at each partner university. Nonetheless, the panel found no evidence of deficiencies in local quality assurance systems and assumes that appropriate corrective action is taken whenever issues are identified at course or instructor level. Additionally, some issues relevant to the programme as a whole are communicated through the academic coordinators to the Programme Director. While there were plans to discuss the course evaluations at the consortium level, through the Advisory Board meetings, this does not appear to have happened. Furthermore, the cooperation agreement recommended establishing an 'Internal and External Evaluation Operational Committee', but this has not yet been implemented. The panel therefore recommends that the consortium establish a formalised quality assurance process at the consortium level, through which all relevant quality assurance data and processes from the partner universities, such as identified issues, corrective measures, and ongoing evaluations, are systematically communicated. This would enable the consortium to take coordinated action whenever cross-institutional issues arise.

The alumni survey, distributed in French, may have limited participation from some international graduates. Nevertheless, the responses indicate that the majority of alumni have successfully secured employment, while non-EU graduates appear to face greater challenges entering the European cybersecurity labour market.

The survey sent to those working in the field provided useful feedback on the scope and content of the programme. The feedback was broadly positive, and some topics for additional courses were identified.

However, the panel notes that the participating universities do not currently have formal processes for the peer review of examinations by academic colleagues or programme management teams.

Overall, the panel concludes that programme pays sufficient attention to quality assurance while delegating a substantial part of the responsibilities to individual partner universities. The panel recommends strengthening quality assurance processes at the consortium level and making greater use of the alumni and industry networks to gather additional feedback on the programme. Doing so would improve coordination between the universities and further enhance both local and joint quality assurance practices.

IV. CONCLUSION

The Erasmus Mundus CYBERUS Joint Master's programme is jointly designed and delivered by three universities: UBS (*Université de Bretagne Sud*), UL (University of Luxembourg) and ULB (*Université Libre de Bruxelles*). At a time of a global shortage of cybersecurity experts, the consortium provides a timely and well-conceived response to an urgent societal and industrial need. The terms and conditions of the collaboration are clearly defined and documented in detail within a Consortium Agreement. The panel concludes that the eligibility requirements for the participating institutions and the degrees are fully met.

The panel finds that the programme's learning outcomes are consistent with the Framework for Qualifications in the European Higher Education Area (FQ-EHEA), and are appropriate for a master's degree in cybersecurity. The panel suggests expanding on the programme's interdisciplinary aspects of the curriculum and position it explicitly in relation to existing international cybersecurity educational frameworks. Graduates are well prepared for employment in industry or for pursuing doctoral studies. The panel also encourages the consortium to offer support for students wishing to obtain professional cybersecurity certifications.

The CYBERUS programme is a two-year master's degree (120 ECTS) that is well-structured, balanced, and demonstrates a clear academic progression from fundamentals to advanced applications. The integrated European mobility component adds substantial value, providing students with exposure to multiple academic and cultural environments. The panel has made some suggestions to update and streamline the curriculum. The allocation of credits and workload is consistent with European standards. Although demanding, the programme remains fully achievable within the expected timeframe.

The admission process is transparent, selective, and consistent with the level and discipline of the programme. It successfully attracts high-potential students from diverse backgrounds and achieves a notably balanced gender representation. The recognition procedures between the partner institutions are compliant with European standards and ensure seamless academic mobility.

The curriculum is up-to-date, well-balanced, and aligned with the intended learning outcomes. The panel recommends the development of peer-to-peer learning initiatives and the establishment of structured collaborations with alumni, who could contribute to further mentoring and professional engagement.

The assessment system employs a wide range of methods and is generally effective. The quality of the master's thesis demonstrates that students are well prepared for professional and research careers. The panel recommends creating a mapping between assessment methods and learning outcomes, and improving and the consistency and timeless of feedback provided to students.

The student support services are comprehensive, well-integrated, and demonstrably contribute to the achievement of learning outcomes. By addressing mobility-specific challenges supporting employability through internships, and fostering inclusion and well-being, the programme ensures that students can succeed both academically and professionally.

The academic and management staff are highly qualified, motivated, and effective. However, the management structure outlined in the Consortium Agreement has not yet been fully implemented. Internal communication between partners functions well, but the panel recommends its further formalisation. The panel also recommends the consortium to expand collaborations with associated partners and to improve the training of external teaching staff. While the facilities and services are sufficient to support the learning activities effectively, the panel recommends exploring opportunities for additional access to key cybersecurity tools used in industry.

The programme's documentation and information management are transparent and comprehensive across all areas, including admissions, curriculum, assessment, and quality processes. Students are consistently well informed and supported throughout their studies.

The programme pays sufficient attention to quality assurance while delegating a substantial part of the responsibilities to the participating universities. The panel recommends to further strengthen the quality assurance processes at the consortium level, and to leverage more the network of alumni and industry to collect

additional information. This would improve coordination between the universities and further strengthen the quality assurance processes further.

The table below summarises the level of compliance of each standard and the overall compliance of the joint programme with the European Approach for quality assurance of joint programmes.

Standard	Assessment
1. Eligibility	Compliant
2. Learning outcomes	Compliant
3. Study programme	Compliant
4. Admission and recognition	Compliant
5. Learning, teaching and assessment	Compliant with conditions
6. Student support	Compliant
7. Resources	Compliant
8. Transparency and documentation	Compliant
9 Quality assurance	Compliant with conditions
Programme as a whole	Compliant

STRENGTHS

- High quality and up-to-date programme in a field with strong market demand
- Highly motivated and competent teaching and management staff
- Selective admission process resulting in a high-quality and diverse student body
- Graduates are well prepared for their future careers
- Strong international mobility opportunities
- Excellent support for students in managing administrative and logistical matters
- Culture of open collaboration benefiting all three participating universities

WEAKNESSES

- Absence of integrated quality assurance processes across the three universities
- Lack of mapping between course assessments and learning outcomes
- No structured alumni network or formalised programme for associated partners
- Communication management and stakeholder engagement remains insufficiently formalised

RECOMMENDATIONS

- Establish a formal quality assurance framework at consortium level, ensuring that all relevant information from each university's internal quality assurance processes (identified issues, remediation measures, on-going evaluations) is shared and coordinated.
- Ensure that students undertaking internships in research laboratories achieve all intended learning outcomes.
- Develop a clear mapping of assessments for each course in relation to the programme's learning outcomes.
- Formalise and strengthen communication channels with all stakeholders, both internal and external.
- Increase student access to key cybersecurity tools used in industry.
- Expand and document feedback mechanisms for all course assessments.
- Establish a formal programme for associated partners and explore opportunities for alumni engagement in various roles.
- Position the programme within international cybersecurity education frameworks.
- enhance the training provided to external teaching staff.
- Review the learning outcomes to reflect developments in Artificial Intelligence and to reinforce the programme's interdisciplinary approach.
- Consider offering support for professional certification to students who request it.

V. COMMENTS OF THE INSTITUTION

Lorient, Brussels, Luxembourg, 24 November 2025

Prof. Jean Peeters
CYBERUS Erasmus Mundus Master Director
Université Bretagne Sud
4 Rue Jean Zay
56100 Lorient

to
Hcéres
Haut Conseil de l'évaluation de la recherche et de l'enseignement supérieur
19 rue Poissonnière
75002 Paris

Subject: Hcéres evaluation of CYBERUS

Dear Hcéres President,

On behalf of the CYBERUS consortium, I would like to thank Hcéres for conducting an audit of the CYBERUS Erasmus Mundus Master in cybersecurity based on the *European Approach for Quality Assurance of Joint Programmes*. We are also grateful for recommending that the programme should be accredited for 6 years.

Legally speaking, this evaluation was not needed as all three universities involved – Université Bretagne Sud (full partner and coordinator), Université Libre de Bruxelles (full partner) and Université du Luxembourg (full partner) – are already accredited in their own countries to deliver the master.

However, we knew it is no easy task to jointly design and implement an Erasmus Mundus master. This is why, with a view to improving the programme's quality and in line with EU guidelines, we requested Hcéres to carry out an independent review.

The findings are in line with many of the comments that we made in the self-evaluation report, prior to the committee's online visit. It confirms that the master is fully compliant the *Standards and Guidelines for Quality Assurance in the European Higher Education Area* (ESG).

Of course, areas of improvement have been identified in the report. Aligning different academic and administrative processes, even in rather similar higher education systems, and keeping up with the best EU practices can be a challenge at times. But the recommendations will be taken into account in the current delivery of CYBERUS and also in the new Erasmus Mundus master's submission. If Erasmus Mundus masters are to be 'programmes of excellence and should contribute to the integration and internationalisation of the European Higher Education Area', as stated in the *Erasmus + Guide*, then they should lead the way and spearhead quality programmes across the EU. This is CYBERUS's intent and purpose.

Yours faithfully.

Prof. Jean PEETERS

With the support of the Erasmus+ Programme of the European Union

European Approach for Quality Assurance of Joint Programmes

ACCREDITATION PROPOSAL

CYBERUS Erasmus Mundus Master in Cybersecurity

Université Bretagne Sud (France)
Université libre de Bruxelles (Belgium)
University of Luxembourg (Luxembourg)

OCTOBER 2025

High Council for the evaluation of research and higher education

SCOPE OF THE PROPOSAL

The Erasmus Mundus Joint Master CYBERUS – Erasmus Mundus master in cybersecurity consortium has mandated the Hcéres to carry out the evaluation of its joint master's programme. The consortium is composed of the following universities:

- Université Bretagne Sud (France)
- Université libre de Bruxelles (Belgium)
- University of Luxembourg (Luxembourg)

The evaluation was conducted in accordance with the European Approach for Quality Assurance of Joint Programmes[1], adopted in May 2015 by the Ministers of the European Higher Education Area, and is fully compliant with the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG)[2].

Following a thorough evaluation process coordinated by Hcéres, the expert panel recommends the award of full accreditation to the Erasmus Mundus Joint Master CYBERUS for a period of six years.

The table below summarises the level of compliance of each standard and the overall compliance of the joint programme with the *European Approach for quality assurance of joint programmes.*

Standard	Assessment
1. Eligibility	Compliant
2. Learning outcomes	Compliant
3. Study programme	Compliant
4. Admission and recognition	Compliant
5. Learning, teaching and assessment	Compliant with conditions
6. Student support	Compliant
7. Ressources	Compliant
8. Transparency and documentation	Compliant
9 Quality assurance	Compliant with conditions
Programme as a whole	Compliant

Hcéres will communicate the evaluation report, together with the accreditation decision, to the quality assurance agencies of the countries represented in the CYBERUS Joint Master. Hcéres has also invited the consortium to contact the relevant national or regional accreditation bodies to determine the procedures required for acceptance of this accreditation decision.

The following strengths, weaknesses, and recommendations are provided to support further improvement of the programme:

STRENGTHS

- High quality and up-to-date programme in a field with strong market demand
- Highly motivated and competent teaching and management staff
- Selective admission process resulting in a high-quality and diverse student body
- Graduates are well prepared for their future careers
- Strong international mobility opportunities
- Excellent support for students in managing administrative and logistical matters
- Culture of open collaboration benefiting all three participating universities

WEAKNESSES

- Absence of integrated quality assurance processes across the three universities
- Lack of mapping between course assessments and learning outcomes
- No structured alumni network or formalised programme for associated partners
- Communication management and stakeholder engagement remains insufficiently formalised

[1] https://www.eqar.eu/assets/uploads/2018/04/02_European_Approach_QA_of_Joint_Programmes_v1_0.pdf
2 https://www.enqa.eu/wp-content/uploads/2015/11/ESG_2015.pdf

RECOMMENDATIONS

- Establish a formal quality assurance framework at consortium level, ensuring that all relevant information from each university's internal quality assurance processes (identified issues, remediation measures, ongoing evaluations) is shared and coordinated.
- Ensure that students undertaking internships in research laboratories achieve all intended learning outcomes.
- Develop a clear mapping of assessments for each course in relation to the programme's learning outcomes.
- Formalise and strengthen communication channels with all stakeholders, both internal and external.
- Increase student access to key cybersecurity tools used in industry.
- Expand and document feedback mechanisms for all course assessments.
- Establish a formal programme for associated partners and explore opportunities for alumni engagement in various roles.
- Position the programme within international cybersecurity education frameworks.
- enhance the training provided to external teaching staff.
- Review the learning outcomes to reflect developments in Artificial Inteligence and to reinforce the programme's interdisciplinary approach.
- Consider offering support for professional certification to students who request it.

This decision, together with the evaluation report, will be published on the Hcéres website.

The evaluation reports of Hceres
are available online : www.hceres.fr/en

Evaluation of higher education and research institutions
Evaluation of research
Evaluation of academic programmes
Evaluation of research bodies
International evaluation and accreditation

Evaluation · Research · Higher Education
Hcéres

19 rue Poissonnière
75002 Paris, France
+33 1 89 97 44 00