MASTER OF SCIENCE IN CYBERSECURITY

KATHOLIEKE UNIVERSITEIT LEUVEN

ACCREDITATION CONDUCT-TAILORED • ASSESSMENT REPORT

15 MAY 2025

S. KATZENBEISSER (CHAIR) • E. OSWALD, A. MATEJIC, J. TEERHUIS (PANEL MEMBERS) •
A.DETANT (SECRETARY) • M. FREDERIKS (PROCESS COORDINATOR)

Table of contents

1 Executive summary

The panel commends the programme management for providing a clear and transparent self-evaluation report (SER), organized in light of three questions that describe the Advanced Master of Science in Cybersecurity in all its aspects: (1) What does the programme intend? (2) How does the programme realise its intentions? and (3) How is the achievement of these intentions demonstrated? To answer these questions, the SER gave well-structured information, that was further discussed with Faculty and programme management, teaching staff, students, alumni and representatives from the professional field.

The one-year, English taught Master programme on cybersecurity is unique in Flanders. It offers international and local Master students interested in the field, a research-based education to tackle the challenges of developing secure digital systems and services. The programme responds to a clear demand for engineers and cyber experts who are able to design and innovate in securing ICT solutions in various sectors.

The challenging technical focus of the programme is complemented with courses on regulatory and management aspects. Overall, the interdisciplinary approach allows excellent and motivated Master students to obtain a wide understanding of cybersecurity, as well as focus on specific technical aspects that interest them. The curriculum is built around 5 pillars, that have been selected to play to the international research strengths of KU Leuven.

The site-visit allowed the panel to appreciate the strong 'personalised approach' in the programme. The small scale of the programme, its strong interactive approach for teaching and assessment, and the straightforward communication between students and teaching staff allow close monitoring of students' progress. Moreover, clear information to students makes it possible to select at a high entry level. At the same time, an early start for preparing students for the Master thesis, and some facilities and flexibility when needed due to a diverse background of the student population, support students to make the most out of their enrolment in the Advanced Master programme.

The panel encourages the programme management to preserve the personalised approach, though it could scale up and attract a few more students. Given the high demand from the professional field, there is room for more graduates. Also, some more diversity in the student population can bring added value, as shown in the feedback received with regard to the involvement of few students with relevant work experience.

The Hague, 15 May 2025

On behalf of the expert panel convened to assess the Master of Science in Cybersecurity

Prof. Dr. S. Katzenbeisser
(chair)

A. Detant
(secretary)

2 Examination of the panel

Since September 2022 the Faculty of Engineering Science at KU Leuven teaches the Advanced Master in Cybersecurity (ManaMa). The one-year programme is the result of a collaboration between two prominent research units from the university: *COSIC* in the Department of Electrical Engineering and *DistriNet* in the Department of Computer Science. Both groups perform internationally renowned research in cybersecurity.

The panel studied the Self-evaluation Report (SER) of the Master of Science in Cybersecurity and its annexes, the general information provided on the website of the KU Leuven, as well as the additional information provided during the site-visit.

The panel commends the Faculty of Engineering Science for providing a clear and transparent SER. Three coherent questions well describe the Advanced Master of Science in Cybersecurity in all its aspects: (1) What does the programme intend? (2) How does the programme realise its intentions? and (3) How is the achievement of these intentions demonstrated? The fourth section of the SER presents an evaluation, focusing on the curriculum design process, the input by industry stakeholders and the trajectory of students admitted to the programme.

The panel has found the SER useful to obtain a good insight in the programme objectives, the learning outcomes set forward, the target audience and admission procedure (chapter 'Profile and Vision'). Further, the SER describes well how the programme is structured, indicating clearly the alignment of courses and learning outcomes; it provides good information on the faculty that is teaching the programme, the teaching formats applied, as well as the infrastructure and services provided to the students (chapter 'Realisation'). The panel found the SER also informative to understand the process of assessments of and feedback by students (chapter 'Assessment'). Lastly, in the chapter 'Evaluation' the panel got a good insight in the choices made for the design of the curriculum, the applications and registrations of the students for the first three academic years of the programme, and the system of quality assurance, based on the COBRA quality assurance agreement at KU Leuven. The panel also appreciated the self-critical reflection in the concluding paragraphs of the SER.

The above listed aspects were subject of the exchanges during the site-visit, where the panel held discussions with the Faculty and programme management, teaching staff, students, alumni and representatives of the work field. The exchanges confirmed the good impressions of the panel and allowed to clarify a number of doubts regarding programme structure and flexibility, course content and integration of new topics, admission of international students, the position on the admission of students with work experience, and the involvement of alumni and the work field in the programme.

2.1 Programme objectives – what does the programme intend?

The cybersecurity programme is unique in Flanders. It aims at instructing and training students on state-of-the-art knowledge and techniques in cybersecurity. The Advanced Master programme offers Master students interested in the field a research-based education to tackle the challenges of developing secure digital systems and services. The goal is to prepare them for several career paths in the domain of cybersecurity, in a technical industrial environment, the public sector or service sector (including telecommunications, finance, insurance, eHealth and industry automation).

The exchanges with alumni and work field representatives confirmed that the programme responds to a clear demand for engineers and cyber experts who are able to design and innovate in securing ICT solutions in various sectors; from securing private data in health applications through to securing the industrial control systems used in the power grid.

It is anticipated by the programme management that some students will start a PhD in cybersecurity; though a career in research or towards the creation of a spin-off company are secondary objectives of the Advanced Master programme.

The technical choices offered in the curriculum are a unique selling point, whereby it was affirmed that the pillars have been selected to play to the international research strengths of KU Leuven. The panel confirms that the excellent research expertise in the Faculty of Engineering Science is a strength that underpins the Advanced Master programme and offers the broadness and in-depth knowledge necessary to cover the technical subdisciplines. The tight links of the curriculum to the internationally renowned research of the Faculty allows the students to specialise in one or more of the research-driven aspects of cybersecurity.

The domain-specific learning outcomes have been inspired by the CyBoK overview of cybersecurity developed in the United Kingdom for master's courses in cybersecurity. The programme aims to cover the majority of these areas but gives specific focus to the more technical aspects and offers the necessary background in legal and cybersecurity management, needed for all cybersecurity professionals. The panel finds this choice well substantiated and in line with the objectives and focus of the Advanced Master.

From the discussions with the programme management, it became clear that the English taught programme targets first international students and, to a lesser degree, students with a master's degree from a Belgian university. The Advanced Master offers a multidisciplinary approach to the field, and targets students with a profound knowledge level coming from a variety of backgrounds, including electronic engineering, computer science, and mathematics. The Advanced Master programme builds upon the prior knowledge and Master level of the students and aims to train them in technical areas underpinning cybersecurity, including cryptographic techniques, software and hardware security, infrastructure and systems security. It also aims to equip them with a 'life-long learning' attitude to adapt to new demands and needs in the work field.

2.2 Realisation

Based on the SER, the exchanges during the site-visit and the additional information studied, the panel found a well-focused programme, that offers Master students a strong advanced technical knowledge in the science of cybersecurity, and additional specialisation opportunities in the proposed pillars. In addition, all students are also exposed to social-technical aspects of cybersecurity, including security management and legal/privacy aspects.

The programme allows students to select four out of five technical pillars that will guide and orient their study focus, in addition to the basics needed by all Cyber professionals (technical, legal and managerial).

The variety in scientific background of students admitted, can bring difficulties for some of the courses if background knowledge and understanding is insufficient or weak (e.g. in the area of Hardware design, which is not part of all computer science curricula). This makes the

programme even more challenging. However, contrary to the somewhat static structure found in the description of the pillars, the panel has been reassured that the structure of the curriculum offers enough broadness and room for flexibility to allow the students to tailor the programme to their background knowledge, needs and interest. Also, overall, the students admitted are very motivated and committed to go the extra mile to succeed this programme.

Certain courses, like the 'capita selecta Computer science' and practical assignments allow for new topics and items to be introduced, discussed and researched by the students. The strong links with the ongoing research in the faculty and the involvement of guest lecturers also allow to bring in state-of-the art knowledge and bring the dynamics in the field into the education programme.

The discussion with students confirmed to the panel that the programme is well-conceived, up-to-date and balanced, with clear choices and sufficient options to tailor it to student's individual needs. The challenging nature is a mere motivation for those enrolled; it is rarely found to be an obstacle.

The site-visit also allowed the panel to understand the strong 'personalised approach' in the programme, whereby communication lines between students and teaching staff are open and regular. Well-reasoned applications by students can be honoured to allow them to take up a limited number of courses outside of the standard curriculum of the Advanced Master (e.g. entrepreneurship). From the SER it was not so clear that students also have options available to follow courses that bring them up-to-speed in the first semester, if needed, and provide them with the required background knowledge to successfully continue at the Advanced Master level. Other ways to facilitate students to 'catch up' is the provision of additional material for self-study. The panel notes that overall, information to students is clear and sufficient, and some facilities and flexibility are provided to allow students to make the most out of their enrolment in the Advanced Master program.

The relatively small scale of the programme was discussed on several occasions during the site-visit. In order to allow close monitoring of students' progress and early detection of potential problems, and to maintain the interactive character of the teaching and learning process, the small scale of the programme is not only an advantage. It appears as a condition that the programme management and teaching staff would want to preserve. The panel agrees with management and teaching staff that the small-scale programme allows the personalised approach towards students, with intense lines between research and education. It also stimulates the group cohesion, which is very appreciated amongst students.

The ambition of the programme management is therefore to position the Advanced Master as a small-scale programme of around 40 students; to build upon the reputation of excellence and attract only very motivated and sufficiently qualified Master students to obtain in this programme a more specialised and in-depth training in the field of cybersecurity.

The panel understood that the admission procedure is strict for international students, requiring not only a Master's level in Engineering, ICT, mathematics or related fields. The management targets a selection of the best international students.

The application is processed first by the International Office of the KU Leuven. An admission committee to the Advanced master programme takes this input and evaluates the full

application including educational level and background. During the site-visit it was confirmed that admission is based on the full application that includes contents of the first master's programme, the grades, the reputation of the previous institute, the results of any GRE test and English language proficiency test, reference letters and the motivation letter of the candidate. For students with a Belgian degree, grades and motivation are also verified to ensure that those who are admitted have all their chances to successfully finish the Advanced Master programme. The panel understands that this strict selection approach by the programme management allows to keep the entry level high.

As the Advanced Master is positioned outside of the regular budgetary framework of educational programmes at university, financial aspects are not a main driver for the Faculty and programme management to target larger student cohorts. Yet, the panel heard the concern from local, Belgian students that a substantial raise of the entrance fees for this programme could become an issue that blocks motivated Master graduates to enrol in the Advanced Master. The panel advises the Management to listen to this concern and examine how the talents of excellent and motivated, but less well-off local students can be allowed into the programme.

For the promotion of the Advanced Master and the recruitment abroad, the programme management counts on the support by the central services. The panel understood that the level of support and promotion by central services could be reinforced to ensure more applications by the best students abroad. As an example, the programme management identifies possibilities for stronger promotion, more applications and possible more admissions of excellent students coming from Eastern European universities.

The panel advises the university management to instruct its central services to invest enough time and resources in promoting the Advanced Master programme, that showcases the quality of the educational programme and research capacity available in the Faculty.
The panel sees that the programme management also uses its own, direct networks with top peers in the world to actively recruit suitable candidates abroad. In the longer run, the programme management also expects a lot in this regard from its own alumni, who can be excellent ambassadors to promote the programme.

The panel not only learned about the social events organised, that bring together students and alumni, but also about the LinkedIn-group that has been set-up to keep trace of the alumni and have a continuous platform to promote research outcomes or relevant events in the domain. The panel appreciates these efforts to build up and maintain the community.

At the same time the panel discussed the tensions raised by a growing demand to allow people with work experience and professional occupations into the programme. The panel learned that the full-time programme as it has been designed and is implemented, did not envisage to attract this type of students. Based on growing demands and some strong applications of few motivated candidates from the work field, the first steps have been set in this direction.

The programme management explained to the panel that more - though limited - admissions of working students could be possible, as long as they are available to attend particular classes and labs and can have a sufficient presence on campus to integrate into the community of students of the Advanced Master. Also, from the exchange with student

representatives and alumni it showed that the presence of students with work experience can bring added value and interesting new perspectives into the labs and interactive group work.

The panel sees some potential here for the Advanced Master to grow and to further enrich the student experience by bringing in this diversity; it advises therefore to carefully examine how this can be done wisely. At the same time the panel understands the concerns of the management to ensure that the personalized and interactive approach can be maintained. Also, in terms of managing resources, the panel sees that no special facilities will be offered to working students.

Moreover, the monitoring of study efficiency in the Faculty is strict and is taken as a criterion for measuring success. The programme management expects all students, also those working, to be sufficiently present on campus and succeed in the courses for which they enrol. Students active in the work field are allowed to spread the course load/credits taken up over a longer period and finish the Advanced Master in two years instead of one. The panel sees this as a reasonable option to accommodate requests to admit students working in the field.

2.3 Demonstration of achievements

The Advanced Master programme adopts a variety of teaching and assessment forms to challenge its students. The courses are taught using a combination of traditional lectures and more activating learning approaches. Most courses also have interactive exercise sessions, in which students are expected to collaborate on solving problems and ask questions. The courses with parts focused on practical aspects are backed up with practical sessions in labs.

Students expressed their appreciation for the variety of learning approaches and mentioned the labs and group work as opportunities to cooperate and learn from the others. The panel also took note of the overall positive feedback of students and alumni with regard to the invitation of guest lecturers from industry or academia in some of the courses. While some guest lecturers are not necessarily the best teachers, students find the integration of real work field expertise and hands-on problems from the industry and public sector stimulating.

The Master of Cybersecurity also uses a broad mix of evaluation activities or assessment forms. For several courses, a written and/or oral exam during the examination period is incorporated as evaluation activity. Some courses contain lab sessions during which students gain hands-on experience with the relevant software or hardware. Participation during contact hours is explicitly evaluated. Students are expected to play an active role and should show the right attitude in order to acquire the desired skills.

From the exchanges with students and alumni, it appears that information on the course content and evaluation methods is transparent and clear. The initial one-week introductory programme combined with a small project, based on a case study, serves the purpose to introduce students to the five major themes/pillars in the curriculum. Students confirmed that this week is much appreciated as it allows them to connect to others in the programme and learn from each other, as the backgrounds of the group members are diverse. The introductory week also offers the insight that is needed to make an informed decision as to which tracks to select. Moreover, students are provided with sufficient information; they know what to expect and appreciate the variety of assessment forms to demonstrate their progress and achievement of the learning outcomes.

When issues arise, they have a voice via student representatives in the Programme Committee. From the site-visit the panel has understood that the Programme Committee plays an important role in ensuring the monitoring of processes and outcomes of the programme. The Programme Committee is the main forum to follow up the quality of the programme, including the teaching and assessment. It plans evaluations, reviews all feedback received and decides on appropriate actions. The students confirmed during the site-visit that this system works well, and their voices are heard.

The programme management indicated that small changes can be easily accommodated in the pillars, adapting the content of some courses and practical assignments. For more substantial changes (e.g. changing the ECTS, adding a new course), the system is slow and more rigid. In a dynamic and fast changing domain like cybersecurity, it could be helpful to allow more flexibility to adapt the programme when necessary.

The panel also learned that in the timeframe between startup and accreditation of the Advanced Master, most aspects of the COBRA quality assurance cycle of the University have been implemented by the programme management and were tailored to the needs of a new programme. The panel appreciates the efforts done to integrate quality assurance processes in the Advanced Master. It is however somewhat surprised to hear that the Advanced Master is not automatically integrated in the university-wide processes. More support by central services to support the programme management in this regard could be useful.

The panel has seen several master theses and finds these of good quality and in proportion to what can be expected given the attributed workload (15 ECTS). The master's thesis finalises the learning pathway on problem solving and design within the context of a cybersecurity problem. It is positive that the programme management adapted its approach, following student feedback. Selecting a master's thesis topic now begins at the start of the first semester. The early kick-off allows students to reflect and start working on their subject, and supports a timely delivery of the thesis. The list of marks that the panel could consult confirms that grades are overall at a good level, and failure rates in the Advanced Master programme are low.

The personalised approach adopted in the programme, is also valid for the master thesis. "Research managers" and "research experts", many of whom have publication records and expertise equivalent to professors at other universities, often help with teaching, proposing and supervising master's projects or giving specialist lectures. In addition, the programme makes use of a large cohort of traditional postdoctoral researchers and PhD students, which help with daily supervision of master's theses, specific advanced lectures, hands-on sessions and lab/exercise sessions. The students appreciate the support mechanisms available and value the close links of the education programme with ongoing research. They also value that many of the topics for the Master thesis are connected to real-life problems, relevant for the work field.

Interesting is that the exchange with the work field representatives revealed a willingness and an engagement to be more closely involved in the delivery of the Advanced Master programme, not only as guest lecturers, but also in the proposal of thesis topics and the monitoring of students with regard to their Master thesis. The programme management could take advantage of this offer to strengthen ties with industry and public sector employers, relevant for the domain.

3 Judgement

Based on the information in the SER and the exchanges during the site-visit, the panel comes to a positive conclusion on all aspects of the Advanced Master programme: Master of science in Cybersecurity.

Overall, the panel confirms that the programme has set clear objectives and learning outcomes, that are translated into a challenging, technically focused programme on cybersecurity. The technical focus is a unique selling point of this programme. In addition, all students are also exposed to social-technical aspects of cybersecurity, including security management and legal/privacy aspects.

The Advanced Master programme offers excellent and motivated Master students in the fields of engineering, maths, IT and related domains, a research-based education to tackle the challenges of developing secure digital systems and services. The tight links of the curriculum to the internationally renowned research of the Faculty allows the students to specialise in one or more of the research-driven aspects of cybersecurity.

The curriculum responds to needs in the professional field (industry, public sector, services) for highly skilled cyber experts; it fulfils its promises and is in line with what students, alumni and work field expect from an Advanced Master programme in the domain.

With regard to the pillar structure and course content, the panel has seen that the structure of the curriculum allows to integrate new elements and topics into the programme. It offers enough broadness and room for flexibility to be tailored to the student's specific interests and background. For students who have already covered material in prior degree courses a flexible approach is adopted to ensure that they gain fully from their educational experience.

The close links of the programme with the research expertise of the staff, and the involvement of guest lecturers from industry and public sectors, are a strong factor that attracts and stimulates students. The small, human-scale of the programme, the efforts to ensure the close ties between teaching staff and students, and the engagement of students (and alumni) in a community of domain experts is fruitful. It not only brings high success rates to the study path of enrolled students; it also helps to bring in expertise and needs from the work field, ensures that the latest state-of the art knowledge is offered to students, and contributes to promoting the programme to new, potential students.

The personalised approach adopted in the programme, is also valid for the master thesis. The panel confirms that these are of good quality and in line with the Advanced Master level.
The panel is confident that programme management will do all the necessary to keep up the high level of education in a growing programme that holds on to a 'personalised approach'. More promotion abroad could facilitate additional recruitment of the best international students. The panel appreciates the strict but fair selection of excellent students that can take benefit of what the programme has to offer and have all chances of succeeding.
The panel sees some potential for the Advanced Master to grow, also in allowing few students with work experience in the programme. These can bring added value and new perspectives to the labs and group work. In order to further enrich the student experience by bringing in this diversity, the panel advises the management to carefully examine how this can be done wisely.

From the information collected and the discussion sessions during the site-visit, some small recommendations can be made:

- While the programme may grow a bit over the coming years, the panel advises to keep the current 'personalised approach', which limits the number of students that can be admitted.
- Given the diverse background knowledge of students, in some cases 'catching up' to the acquired level at the start is necessary for students to successfully take all the courses of the Advanced Master. The panel advises to make it more explicit to admitted students what are the facilities offered to support them (additional material for self-study, crash-courses, taking up classes outside of the regular programme).
- The panel advises the University management to integrate the Advanced Master programme in the regular processes and support schemes of the university and its central services, so as to offer more administrative support and more investment in the promotion of the programme abroad.
- The panel advises to adopt more flexibility for introducing new courses and adapt the Advanced Master programme if needed. A light-weight procedure for introducing changes is particularly useful in domains that are dynamic and fast changing, such as cybersecurity.

4 Review process

The assessment was carried out in line with the 'Assessment framework programme accreditation customised to own conduct' (June 2020), of the QUALITY ASSURANCE SYSTEM FLANDERS 2019-2025.

The panel prepared itself for the assessment on the basis of the information file submitted by the institution when applying for accreditation. Prior to the preparatory meeting of the panel, each panel member formulated initial impressions and questions were listed. During a preparatory online meeting on 24 March 2025, the panel discussed all information received in the application file and prepared the dialogue with the programme. Impressions and questions were updated before the first dialogue with the institution, during a preparatory meeting on 10 April 2025.

An on-site dialogue took place on 11 April 2025 with representatives of the management, the Dean of the Faculty of Engineering Science, the Chair of the Department of Electrical Engineering, the programme development team and teaching staff, students, alumni and representatives of the work field (see Annex 4).

During the dialogue the panel investigated the context of the programme and the institution and collected all required information to make a judgement on the quality of the programme.

During a closed meeting of the panel at the end of the site-visit the panel discussed all information obtained and translated it into a holistic judgement. The panel took this conclusion in full independence.

All information obtained led to a draft assessment report that has been sent to all panel members. The feedback from the panel members has been processed. The assessment report adopted by the chairman was submitted to NVAO on 15 May 2025.

Annex 1: Administrative data regarding the institution and the programme

Institution	Katholieke Universiteit Leuven
Address, institution website	Oude Markt 13, 3000 Leuven https://www.kuleuven.be
Status institution	Publicly funded higher education institution
Programme	Master of Science in Cybersecurity
Level and orientation	Advanced Master (ManaMa)
(Additional) title	-
(Parts of) field of study(s)	Engineering
Specialisations	-
Programme routes	-
Location where the programme is offered	Leuven
Teaching language	English
Study load (in credits)	60 ECTS
New training in Flanders	No
Programme-specific learning outcomes	Yes
Connecting options and potential further education	-

Annex 2: Programme-specific learning outcomes

Table 1: Mapping of the Programme- onto the Domain-specific outcomes

Domain-specific learning outcome	PSLO
1. Possess advanced knowledge and understanding of offensive and defensive techniques, methods and tools in the space of cybersecurity, and of their relevance and applicability in practice.	1,2,12
2. Possess advanced knowledge and understanding of theories, methods and tools to model processes and systems and apply these to cybersecurity problems.	1,5,6,7
3. Are able to assess vulnerabilities and threats on systems in order to identify weaknesses and risks and to validate cybersecurity solutions.	1, 2, 5, 12
4. Have the knowledge and understanding to develop, deploy and manage cybersecurity protection techniques and tools in collaboration with other cybersecurity experts and with ICT professionals.	12,13,14
5. Are able to independently create (analyse, model and design) solutions for complex problems in cybersecurity research or applications, if appropriate by splitting these up in manageable sub-problems and to critically evaluate the results.	9,11,15, 18
6. Have the required knowledge and understanding of cybersecurity techniques and tools to be able to engage in securing digital services in professional areas such as healthcare, financial services, government, manufacturing, logistics; they are able to independently select appropriate technological means and constructively apply them to a problem in cybersecurity.	24,26
7. Are able to critically identify novel problems and assess proposed solutions in cybersecurity, in full awareness of the potential and limitations of the state of the art.	7,8,10
8. Are able to critically identify novel problems and assess proposed solutions in cybersecurity, in full awareness of the potential and limitations of the state of the art.	4, 7,8,9,10,23
9. Are able to clearly and accurately report on scientific findings in cybersecurity or on advances in its application domains, both in written and in oral form, and are able to critically assess new scientific developments within subdomains of cybersecurity.	20, 21, 22
10. Have a good understanding of the interdisciplinary (including psychological, sociological and economic), regulatory and international dimensions of cybersecurity, taking into account the constraints and the various aspects of the sectors they will be part of as professionals (e.g. government, healthcare, software industry, banking and insurance, production industry etc.).	16, 24
11. Are able to act responsibly from an ethical, legal and professional point of view while taking into account the broader economic and societal context.	11, 17, 25, 26

Annex 3: Composition of the panel

The assessment was made by a panel of experts convened and appointed by the NVAO. The panel is composed as follows:

Prof. Dr. Stefan Katzenbeisser (chair), Chair of Computer Engineering, University of Passau

Prof. Elisabeth Oswald (panel member), Professor of Applied Cryptography, University of Birmingham and Professor of Cybersecurity, University of Klagenfurt

Ana-Maria Matejic (panel member), Director, Client Programs, Nexova Group SA

Julia Teerhuis (student panel member), student Master of Science Computer Security, Vrije Universiteit Amsterdam

The panel was assisted by:

- Mark Frederiks, senior policy advisor NVAO, process coordinator;
- Anja Detant, secretary.

All panel members and the process coordinator/secretary have signed NVAO's code of deontology.

Annex 4: Schedule of the site visit

KU Leuven, ESAT, Campus Heverlee
11 April 2025

Time	Meeting
08:30 – 09:00	Reception, short preparatory panel meeting
09:00 – 09:30	Session 1: Representatives of the university management
09:45 – 11:00	Session 2: Programme management
11:15 – 12:15	Session 3 - Students
12:15 – 13:15	Panel meeting and lunch
13:15 – 14:00	Session 4 - Teaching staff
14:15 – 15:00	Session 5 – Professional field + Alumni
15:15 – 15:45	Second dialogue with program management (if needed)
15:45 – 16:45	Final panel meeting
17.00 – 17:15	Concluding dialogue

Annex 5: Overview of the material studied

Information file

- Self-Evaluation Report – Initial Accreditation

Mandatory annexes to the information file

- Addendum 1: General information on the programme
- Addendum 2: Administrative data of institution and programme

Appendices Self-Evaluation Report Master of Science in Cybersecurity

- Appendix 1: Mapping of the 26 programme-specific learning outcomes (PSLO) map onto the 11 domain-specific learning outcomes (DSLO)
- Appendix 2: List of Master Theses
- Appendix 3: Curriculum Vitae of Lecturers

Documents made available during or leading up to the dialogue

- Examples of Master theses
- Master theses, list of grades and evaluation forms

Annex 6: List of abbreviations

CyBoK	Cyber Security Body of Knowledge
ECTS	European Credit according to the European Credit Transfer and Accumulation System
GRE test	Graduate record examinations test
ManaMa	Advanced Master programme (Master na Master)
NVAO	Accreditation Organisation of the Netherlands and Flanders (Nederlands-Vlaamse Accreditatieorganisatie)
SER	Self-evaluation Report

Colofon

Master of Science in Cybersecurity
Katholieke Universiteit Leuven (VL131117-25)
Accreditation Conduct-tailored • Assessment report
15 May 2025
Composition: NVAO • Vlaanderen

Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 · 2514 JG Den Haag
P.O. Box 85498 · 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net