



M Security and Network Engineering
University of Amsterdam

© 2026 Academion

www.academion.nl
info@academion.nl

Project code P2419

Contents

Summary	4
Score table	5
Introduction.....	6
Procedure.....	6
Panel	7
Information on the programme	7
Description of the assessment.....	8
Organization	8
Recommendations previous panel	8
Standard 1. Intended learning outcomes	8
Standard 2. Teaching-learning environment.....	10
Standard 3. Student assessment	16
Standard 4. Achieved learning outcomes	18
General conclusion	19
Recommendations	19
Appendix 1. Intended learning outcomes	20
Appendix 2. Programme curriculum.....	21
Appendix 3. Programme of the site visit.....	22
Appendix 4. Materials	23

Summary

Standard 1. Intended learning outcomes

The panel found that the master's programme Security and Network Engineering offers a unique profile in combining networking and security in a one-year master's programme, with an appropriate balance between academic and professional skills. It concludes that the ILOs are well designed, relevant and up to date, and reflect the academic orientation and master level of the programme. The programme is well connected to the professional field and uses its input in keeping the ILOs up-to-date. The panel advises to incorporate legal and societal impacts into the ILOs.

Standard 2. Teaching-learning environment

The curriculum is well aligned with the intended learning outcomes, employing a variety of teaching methods that are effective to achieve these goals. The programme is distinguished by its practical, hands-on approach, featuring numerous projects that allow students to explore their own interests, and an ambitious range of topics and skills covered in the curriculum. The panel advises the programme to annually review and include emerging topics in courses, while continuously monitoring developments in security and network engineering, and making strategic choices in collaboration with the Professional Advisory Board to adapt curriculum content as needed. The panel appreciates the opportunity for students to study part-time, which reflects the programme's student-centered approach and enhances its appeal to working professionals. It recommends exploring more flexible arrangements for part-time students to complete the 3-month research project, and that any changes be clearly communicated to part-time students. Teaching the programme in English is appropriate and fully supports the rationale for using English as the language of instruction and in the programme name. The panel concludes that the admission requirements are appropriate and the curriculum is feasible. The panel is very positive about the strong commitment that the programme demonstrates to fostering a welcoming and inclusive environment for students, and the highly qualified and committed teaching staff. The panel recommends monitoring staff workload distribution to ensure it remains manageable for all staff.

Standard 3. Student assessment

The system of assessment in the master Security and Network Engineering is reliable, valid and transparent. Assessment methods are varied, and checks and balances are in place to ensure course and graduation project assessment quality. The Board of Examiners is in control and fulfils all of its legal duties in a satisfactory way. Graduation project assessment is up to standard, with the consistent use of a four-eye principle in grading and the use of an thesis assessment rubric to substantiate the grades. The panel values the oral defence as substantial part of graduation project assessment, which in the opinion of the panel is useful in the light of generative AI and adds to the active learning process of students. The panel advises introducing formal intermediate evaluation dates during the graduation project process to assess student progress.

Standard 4. Achieved learning outcomes

The quality of the graduation projects and the performance of graduates show that students of the MSc Security and Network Engineering realize the programme's intended learning outcomes. The graduation projects, many of which have resulted in academic papers, demonstrate solid research skills and suitably reflect the cybersecurity and networking profile of the programme.

Score table

The panel assesses the programme as follows:

M Security and Network Engineering

Standard 1: Intended learning outcomes	meets the standard
Standard 2: Teaching-learning environment	meets the standard
Standard 3: Student assessment	meets the standard
Standard 4: Achieved learning outcomes	meets the standard
General conclusion	positive

The assessment panel has reviewed the report and agrees with its contents. On behalf of the panel,

Prof. dr. ir. Nele Mentens
Chair
Date: 26 March 2026

Drs. Jessica van Rossum
Secretary

Introduction

Procedure

Assessment

On 6 February 2026 the M Security and Network Engineering of the University of Amsterdam was assessed by an independent peer review panel. The assessment followed the procedure and standards of the NVAO Assessment Framework for the Higher Education Accreditation System of the Netherlands (April 2024).

Quality assurance agency Academion coordinated the assessment upon request of the University of Amsterdam (UvA). Jessica van Rossum acted as coordinator in the cluster assessment and as secretary for the assessment of the programme. She has been certified and registered by the NVAO.

Panel composition

Academion composed the peer review panel in cooperation with the institutions and taking into account the expertise and independence of the members.

On 12 December 2025, the NVAO approved the composition of the panel. The coordinator instructed the panel chair on her role in the site visit according to the Panel chair profile (NVAO 2016) on 14 October 2025.

Preparation

The programme composed a site visit schedule in consultation with the coordinator (see appendix 3). The programme selected representative partners for the various interviews. It also determined that the development dialogue would be made part of the site visit. A separate development report was made based on this dialogue.

The programme provided the secretary with a list of graduates over the period 2023-2025. In consultation with the secretary, the panel chair selected 15 theses. She took the diversity of final grades and examiners into account, as well as the fulltime (11 theses were selected) and parttime variant (4 theses were selected). Prior to the site visit, the programme provided the panel with the theses and the accompanying assessment forms. It also provided the panel with the information file and additional materials (see appendix 4).

The panel members studied the information and sent their findings to the secretary. The secretary collected the panel's questions and remarks in a document and shared this with the panel members. In a preliminary meeting, the panel discussed the initial findings on the information file and the theses, as well as the division of tasks during the site visit. The panel was also informed on the assessment framework, the working method and the planning of the site visits and reports.

Site visit

During the site visit, the panel interviewed various programme representatives (see appendix 3). The panel also offered students and staff members an opportunity for confidential discussion during a consultation hour. No consultation was requested. The panel used the final part of the site visit to discuss its findings in an internal meeting. Afterwards, the panel chair publicly presented the preliminary findings, general observations of the panel and suggestions for development themes.

Report

The secretary wrote a draft report based on the panel's findings and submitted it to an Academion colleague for peer assessment. Subsequently, the secretary sent the report to the panel for feedback. After processing this feedback, the secretary sent the draft report to the programme in order to have it checked for factual irregularities. The secretary discussed the ensuing comments with the panel chair and changes were implemented accordingly. The panel then finalized the report, and the coordinator sent it to the Faculty of Science of the UvA.

Panel

The panel assessing the M Security and Network Engineering of the University of Amsterdam consisted of the following members:

- Prof. dr. ir. N. (Nele) Mentens, Full professor Applied Cryptography and Data Security at the Leiden Institute of Advanced Computer Science of Leiden University, and at the Faculty of Engineering Technology of the KU Leuven [Chair];
- Prof. dr. G. (Georgios) Smaragdakis, Full professor Cyber Security at the Faculty of Electrical Engineering, Mathematics and Computer Science of the TU Delft;
- Dr. ir. E. (Erik) Poll, Associate Professor at the Digital Security Research Group of the Radboud University;
- I. (Imane) el Caïdi BSc, Master student Computer Science (track Algorithmic Design and Analysis & Operations Research) at Utrecht University, [Student member].

Each panel member, the panel secretary and the programme have filled out the Statement of Impartiality and non-disclosure agreement, as required by the NVAO. They can confirm that the assessment was carried out in complete independence.

Information on the programme

Name of the institution:	University of Amsterdam
Address:	Nieuwe Achtergracht 166, 1018 WS Amsterdam
Website:	www.uva.nl
BRIN-number:	21PK
Status of the institution:	Publicly funded institution
Result institutional quality assurance assessment:	Positive
Programme name:	Security and Network Engineering
ISAT number:	60227
Orientation of the programme:	Academic
Level of the programme:	Master (NLQF 6)
Number of credits:	60 EC
Language of instruction:	English
Professional requirements:	no
Specializations or tracks:	no
Location:	Science Park, Amsterdam
Mode(s) of study:	Fulltime, parttime
Awarded degree:	MSc
Submission date NVAO:	1 May 2026

Description of the assessment

Organization

The master's programme Security and Network Engineering (SNE) of the University of Amsterdam (UvA) is organized by the Graduate School of Informatics in the Faculty of Science (FNWI), which organizes eight master's programmes in the computing sciences. Staff associated with the programme is provided by the Informatics Institute (IvI). The programme shares its Programme Committee and Examination Board subcommittee with the MSc Software Engineering. The MSc SNE is part of the Examinations Board Exacte Wetenschappen/Informatiewetenschappen, which is one of two Examination Boards within the faculty.

The programme is housed in both the Science Park 904 building and in the Lab42 building that connects students with the informatics ecosystem in Amsterdam, since it also houses various research labs, start-ups, research institutes and tech-policy organizations.. Educational support is provided by the faculty's Education Service Centre (ESC). The MSc SNE has an influx of approximately 35 students per year.

The programme can be followed in either a full-time or part-time variant. The part-time variant offers the same content as the full-time variant, but is delivered over a longer period. Approximately 20% of students follow the programme part-time, usually because they combine the master's programme with a job. The discussions and conclusions in this report concern both the full-time and part-time variants, unless explicitly indicated otherwise.

Recommendations previous panel

In 2020, the previous accreditation committee provided the programme with several recommendations. These included considering a second programme on security and network modelling, recruiting more lecturers and lab teachers with a solid human resource policy for lab teachers in place, reflecting upon the set-up of the research projects and considering the option of one instead of two research projects, and assessing the research projects in a more consistent manner. The programme presented the actions taken based on these recommendations to the panel. Based on this information and discussions during the site visit, the panel concludes that the recommendations have been taken to heart by the programme. Where relevant, these are discussed in more detail in the respective standard.

Standard 1. Intended learning outcomes

The intended learning outcomes tie in with the level and orientation of the programme; they are geared to the expectations of the professional field, the discipline, and international requirements.

Findings

Profile

The master's programme SNE is a 60 EC academic and professionally oriented programme offered both in a full-time (one year) or part-time (two year) variant. The programme aims to educate experts in the field of security and network engineering. In a world that increasingly uses and depends on ICT infrastructure, and where cyber threats are a major issue, security and network engineers are indispensable in the efficient and effective functioning and innovation of this infrastructure. Their technical expertise in combination with understanding of the goals and needs of organizations and society ensure the correct operation and management of the digital infrastructure. The programme uses a fast-paced learning approach to efficiently

train students to become experts in the field of networking and cybersecurity. The programme is also suited to re-skill existing professionals, who aim to enter or evolve into a network/security role in their current organization, or aim to establish a new professional networking/security trajectory in another organization. The parttime variant provides professionals the opportunity to follow SNE alongside a job.

The focus of the programme lies on both security and networking skills in the professional context, as well as on academic research skills. These skills are offered in three learning trajectories throughout the programme:

1. Network Engineering trajectory, which encompasses skills to integrate a complex networked system, experiment with network technologies and protocols, and build a running network.
2. Security Engineering trajectory, representing skills to analyse basic cryptographic algorithms and constructs, evaluate the security properties of a system or organization, and develop security guidelines for systems using relevant advanced techniques.
3. STEM skills trajectory, representing the research-driven education vision for students being able to create a solution to a research problem, defend their research to a competent audience, reflect on ethical implications of a given problem, and act effectively in academic and/or industrial settings.

The panel has studied the profile of the programme, and considers it to be appropriate and unique in combining networking and security in a one-year master's programme. Moreover, the panel appreciates the balance between academic and professional skills. The emphasis on both professional and research skills position the programme as a valuable asset in addressing the global demand for cybersecurity and networking expertise. The panel appreciates the opportunity the programme offers to combine it with a job.

From the documentation and the interviews during the site visit, the panel learned that the programme management considered the suggestion of the previous panel to offer a second study programme, ultimately deciding to not implement it at this time. The main reasons are primarily human resource limitations and secondarily the fragmentation of the security community inside UvA. The panel understands this decision and agrees with this.

Intended learning outcomes

The programme has translated its profile into seven different intended learning outcomes (ILOs), for which it uses the term Exit Qualifications (EQs; see Appendix 1). The ILOs are formulated alongside the Dublin Descriptors on master's level: Knowledge and understanding, Application of knowledge/ understanding, Formulation of judgement, Communication, and Learning skills. The programme presented an overview to the panel where all ILOs were connected to qualifications related to the Dublin Descriptors on master's level, and to NLQF level 7.

To promote the alignment of the programme's intended learning outcomes with the expectations of the professional fields that students end up in, the programme uses the input of academic and industrial partners, which act as an informal sounding board for the programme management and staff. The programme also has a Professional Advisory Board (PAB) in place, which is part of the Graduate School of Informatics (GSI). This board consists of one senior industry representative per programme, often an alumnus. The PAB meets twice per year with the programme directors of the GSI, and advises the programme about the integration of work field developments into its profile, and ILOs. Furthermore, SNE has developed a strong alumni community that actively contributes to the programme with guest lectures, outreach and industrial connections.

The panel studied the ILOs and their alignment with the academic and professional field. It concludes that the ILOs are well designed, relevant and up to date. They reflect the academic orientation and master's level as described in the NLQF Framework level 7. The panel found that the ILOs are very relevant, more so in preparation for the professional field than the academic field, as is to be expected for a one-year academic master's programme that is strongly aligned with the professional field. The panel concludes that there is ongoing attention to updating exit qualifications and course content, informed by regular discussions with the Professional Advisory Board. This ensures the programme remains relevant and responsive to the professional field. This is complemented with many informal connections of the programme to the professional field. For example, SNE incorporates several guest lectures by professionals from industry, many graduation projects are performed in close collaboration with local and international industry, and the participation and input of working part-time students within the programme contributes to the alignment with the professional field.

The panel noted that, given the critical nature of the field of security and network engineering, the programme's ILOs do not explicitly address legal and societal impacts. As professionals in this domain often operate at the intersection of technology, ethics, and regulatory frameworks, the panel advises the programme to formally incorporate legal and societal considerations into its exit qualifications. This should be clearly documented to reflect the programme's commitment to educating well-rounded professionals who understand the broader implications of their work. The panel appreciates the presence of an ethics course in the programme, which provides students with a foundation beyond technical skills, particularly as they engage in hands-on activities such as ethical hacking. Given that students are also involved in responsibility disclosures (e.g., vulnerability reporting), it is essential that they are equipped with an understanding of legal boundaries, ethical responsibilities, and societal consequences. By explicitly integrating these aspects into the ILOs, the programme will better prepare graduates to navigate the complex ethical and legal landscapes of cybersecurity and network engineering.

Considerations

The panel found that the master's programme Security and Network Engineering offers a unique profile in combining networking and security in a one-year master's programme, with an appropriate balance between academic and professional skills. It concludes that the ILOs are well designed, relevant and up to date, and reflect the academic orientation and master level of the programme. The programme is well connected to the professional field and uses its input in keeping the ILOs up-to-date. The panel advises to incorporate legal and societal impacts into the ILOs.

Conclusion

The panel concludes that the programme meets standard 1.

Standard 2. Teaching-learning environment

The curriculum, the teaching-learning environment and the quality of the teaching staff enable the incoming students to achieve the intended learning outcomes.

Findings

Curriculum and didactics

The curriculum of the MSc Security and Network Engineering consists of 60 EC and comprises of seven mandatory courses, such as Security of Systems and Networks, InterNetworking and Routing, and Cyber Crime and Forensics, and a final thesis. All courses are 6 EC, except the 3-month master thesis, which is 18

EC. Teaching is organized into two semesters of 20 weeks each. A semester consists of three periods of 8, 8 and 4 weeks respectively. In 8-week periods, full-time students typically attend two courses running in parallel, while in 4-week periods, they attend only one course.

The three learning trajectories relate to skills learned within the various courses, namely:

1. Network Engineering trajectory representing the network-related technical content of the programme, i.e. network design, configuration and testing, routing & switching protocols, internet protocols, mobile and wireless networks, network firewalls, intrusion detection systems, network automation, monitoring, and system administration.
2. Security Engineering trajectory representing the security-related technical content of the programme, i.e. ethical hacking, building secure devices, network security, secure protocol design, log analysis, software security, secure coding, security of cyber-physical systems, side-channel attacks, forensics and cryptography.
3. STEM Skills trajectory representing the research-driven education of the SNE programme, i.e. research question formulation, state-of-the-art analysis, hypothesis testing, analytical thought, constructive criticism, problem solving skills, research methods, hacking mindset, system administrator management skills, scientific ethics, intellectual property, open science & technology, data collection, data management, data analysis, statistics, coding skills, academic communication & presentation skills, collaboration skills, and scientific writing skills.

The SNE programme is based on the philosophy that the best results for a 1-year programme can be achieved by a streamlined curriculum, strong group cohesion and active student participation. Students are encouraged to participate actively during lectures, lab sessions and group projects, and collaborate with their lecturers and other students. SNE often attracts students with past work experience in IT, therefore some students already possess detailed knowledge about certain topics, and students can benefit from peer learning. The master's programme aims for a hands-on state-of-the-art educational approach that closely couples theory lectures with follow-up lab sessions and student-driven projects. Students are constantly exposed to state-of-the-art wired and wireless networking devices and other equipment, with a dedicated classroom, dedicated lab rooms and personal workspaces, including desktop and server access. Students are encouraged to contribute to discussions and share their knowledge with the group, take an active role in the learning process, within a professional setting consisting of coworkers that possess various educational and knowledge backgrounds.

The SNE programme uses Open Technology to support the education, deploying Open Source software, hardware and tooling, and following Open Science publishing practices. The open philosophy is also the basis for the SNE lab, which is situated next to the lecture rooms. A dedicated system engineer maintains a state-of-the-art infrastructure that supports new and innovative software and hardware for exploration by the students, while remaining vendor-independent in the educational process. SNE reserves one day each week for organizing colloquia, guest lectures and field trips, which are part of the curriculum although they go beyond individual courses. These events bring forward additional topics that are relevant in the field of networking and security. It gives the students the opportunity to meet speakers from the industry, external organizations and other universities, who give their own view and insight on relevant topics encountered in practice. Several of these speakers originate from the Dutch and international community of networking/security and alumni. Alumni are also actively involved in the formulation and coaching of research projects.

During the 18-EC (3-month) graduation project students pursue an independent research project under the guidance of an academic supervisor. This follows the recommendation of the previous panel to integrate the

two research projects offered at the time into one larger graduation project. In the case of a graduation research projects in industry, , a member of staff is assigned as academic supervisor in order to ensure the academic quality, relevance and significance of the work. The academic supervisor meets the student on a regular basis to discuss progress and provide guidance. Companies hosting students are informed that graduation projects are individual and independent research projects leading to a thesis that is publicly defended, and that it does not encompass an internship.

After studying the curriculum and discussing the curriculum with programme management, students and staff, the panel is of the opinion that the curriculum is well aligned with the intended learning outcomes, employing a variety of teaching methods that are effective in achieving these goals. The learning trajectories serve as a valuable tool for ensuring coherence between courses and the overall programme objectives. According to the panel, bringing together two separate research projects into one 3-month research project is the right choice, especially for fulltime students. The master's programme is distinguished by its practical, hands-on approach, featuring numerous projects that allow students to explore their own interests. According to the panel, this highlights well the student-centredness of the programme; although the programme has a fixed curriculum, there is ample room for students to incorporate individual accents. The panel is impressed that the curriculum covers an ambitious range of topics and skills for a one-year programme, enriched by field trips and contributions from industry guest lecturers. Overall, the programme offers a well-rounded and appealing curriculum for its students.

The panel concludes after interviews with programme management and staff that the programme demonstrates thoughtful deliberation in curriculum design, including decisions on what to include or exclude. The panel acknowledges the rapid pace of developments in security and network engineering and commends the programme's proactive approach to curriculum review. Actual topics such as post-quantum technologies, malware analysis, incident response, risk management, and secure AI are addressed in the programme, primarily through the colloquium. The panel advises to also update the courses annually, continuously paying attention to security and network engineering developments. The programme could collaborate with the Professional Advisory Board to prioritize and adapt curriculum content as needed.

The panel observed that student participation in course evaluations via online questionnaires after the exam remains low, limiting the usefulness of the feedback collected. To increase response rates and gather more meaningful input, the panel advises to plan evaluations earlier in the course, such as during the final lectures—before exams—to focus feedback on the lectures rather than the exam itself. Facilitating lecturers in collecting student feedback earlier in the course could help to enable timely adjustments and improvements. The programme could offer a paper-based option for evaluations, where students complete and submit forms physically. This approach has been shown to improve participation rates. Also, revising and diversifying the questions asked could capture more nuanced feedback. Lastly, the panel encourages the programme to explore alternative modes of evaluation beyond questionnaires to further boost student response.

Part-time variant

The number of part-time students is on average 22% of the student population. Full-time and part-time students follow the same education, with part-time students spreading the course load out over two years. Students in the full-time variant follow two courses per teaching block, whereas part-time students follow one course or project per block. To keep the curriculum content coherent for part-time students, part-time students follow security courses in the first year. In their second year, part-time students follow network and large systems courses. Both year 1 and year 2 start with basic courses on security and networks, and they gradually build up to advanced courses on security and networks. Course lectures and lab sessions are

scheduled on two specific days every week, allowing part-time students to effectively study approximately 2.5 days per week and work 2.5 days per week. Furthermore, part-time students spread the work on the thesis over a longer period to allow them to work on it part-time. There is always an academic supervisor involved in overseeing the graduation project.

The panel appreciates the opportunity for students to study the programme part-time. This speaks for the student centeredness of the programme, and the panel feels that this makes the programme more attractive to students in the professional field. With regard to the 3-month research project, the panel recommends exploring more flexible arrangements for part-time students to complete the project in combination with their professional commitments. To date, part-time students were not always informed about the possibility of completing it over six months. Taking three months from work, is not realistic for most part-time students, and splitting the research project was also not practical, making it hard for part-time students to integrate the research project in their study programme. Possible solutions could be to allow students conducting the research project within their own company, or to offer the option to split the research project across both years of the programme, rather than requiring a continuous three-month block in year 2. The programme management has expressed its intention to introduce this flexibility for part-time students. However, the panel recommends that any changes be clearly communicated to students, as the current structure raises some hurdles for students and transparent communication will help manage expectations and ensure a smoother experience for part-time learners.

Language of instruction

The programme is offered in English and uses an English language name. The field of computer, network, and security engineering is dominated by the English language. Many of the organizations in which graduates can be expected to work, both professional and academic, are situated in an international environment where English is the language of operation. Using the English language prepares students for this context. Furthermore, the English language allows for an international classroom: around 40% of the students is international. The panel concludes that teaching the programme in English is an appropriate choice, and approves of the rationale to use English as language of instruction and in the programme name. It agrees that many organizations are internationally oriented, and that being able to navigate in an English-language environment is an important skill for graduates.

Intake, admission, and feasibility

Students can be admitted to the MSc SNE with a bachelor's degree in Computer Science, (Technical) Informatics or another related degree. This degree can be academic (WO) or from a university of applied sciences (HBO), including comparable foreign qualifications. Applicants must also provide recent proof of their command of the English language based on a UvA standard. Next, applicants must take an intake examination to find out whether they have the necessary basic skills and attitude to participate in the programme. Before the assessment, applicants can study intake exam material available on the master's programmes website, and they can visit the programme as part of the Master's initiative of the UvA. During these occasions they can spend a day with the current students and lecturers and ask questions. The intake examination consists of a number of multiple choice tests on basic knowledge mathematics, networking, programming and reading/writing skills. When all tests are evaluated as sufficient, a student is invited for a personal interview with members of the Admission Board, who decide on the eligibility of the student based on the test results but also on the applicant's motivation.

On average, 47% of students graduates nominally, and 75% within one year delay. During the site visit, the panel discussed feasibility of the programme with students, and learned that over all students perceive the programme as feasible. Mostly, study delay was because of personal reasons, for example combining

studying with a job. Based on student experience and graduation rates, the panel concludes that the admission requirements are appropriate and the curriculum is feasible. It appreciates the entrance exam, which is valued by students and programme management, and contributes to a carefully designed admission process.

Guidance and support

All courses provide contact hours devoted to feedback and guidance. During these contact hours, students typically present or demonstrate intermediate results to teachers and receive feedback on contents and process. Staff members pay attention to analysis, argumentation, and critical evaluation within a safe environment for exploration that also allows failure as a didactic experience. The combination of guided learning and self-study aims to create a learning environment in which students develop independence, creative and critical thinking, whilst safeguarding progress and accuracy of process.

In addition to guidance, coaching and support as part of regular courses, the MSc Security and Network Engineering provides a number initiatives to support student and teacher communication and guide students. The programme starts with a 90-minute welcome session followed by a reception in the week prior to the start of an academic year. During this session, students meet their peers, receive first-hand tips from second-year part-time students and become personally acquainted with key teaching staff and programme management. The details of the programme's internal organization are explained, regulations from course registration to plagiarism and fraud are discussed, and the students are familiarized with the most important online systems and relevant organizational units. In the fall at the end of the first exam week, a 3-day SNE trip to a location that is meaningful for the programme content is organized to build cohesion and trust among students and between students and the teaching team.

The SNE has three dedicated lab rooms next to each other, which students can use for lab sessions and also for socializing moments, encouraging familiarity among peers and with the teaching staff. The programme communicates with students via mailing lists, in the classroom, and makes use of electronic systems, such as Datanose and Canvas. For issues that students experience beyond the course content scope, the GSI has a professional study adviser, who supports students in a variety of matters from monitoring progress to course registration, and general study planning. If a student falls ill, has personal problems or has a functional impairment, the student adviser makes individual arrangements with the student and teachers in order to prevent or minimize delays. If appropriate, the study adviser refers students to a student counsellor, student psychologist or to the Student Careers Centre. The study adviser has weekly office hours on appointment, students can make appointments outside office hours if needed and can contact the study adviser via e-mail or telephone. The programme coordinator is the contact person for all administrative problems a student may have.

The panel is very positive about the strong commitment that the programme demonstrates to fostering a welcoming and inclusive environment for students. Significant effort is invested in making students feel at home and building a positive atmosphere among both students and lecturers. Initiatives such as onboarding activities for new students and the annual fall SNE trip contribute to this supportive community. The well-provided information provision, dedicated teaching spaces and facilities further underscore the programme's student-centred approach, as does the flexibility offered by the part-time study option discussed earlier. This adaptability ensures accessibility and accommodates diverse student needs, including students with a functional impairment. The programme management's dedication and drive is evident, and the close-knit community creates a cohesive and engaging learning experience.

Teaching staff

SNE teaching staff consists of ten members, including lab teachers and an educational technical coordinator, supported by teaching assistants. These are teachers with a temporary four-year contract that fully engage in teaching. They support the other teaching staff members with many supporting teaching activities, as well as coordination and administrative tasks. All staff members are required to obtain a University Teaching Qualification (UTQ; Basis Kwalificatie Onderwijs - BKO). The lecturers are staff members of the research institutes of the UvA such as the Informatics Institute (IvI). They fulfil their teaching tasks on request of the programme director after consultation with the respective directors of the involved research institutes.

The panel is positive about the highly qualified teaching staff of the master's programme SNE and values that each course has at least one lecturer holding a PhD degree, and most lecturers have their UTQ. The staff is well qualified in terms of both research expertise and didactic skills. The alignment with the research institute IvI promotes research-based teaching and alignment between the programme and the research expertise. There are sufficient opportunities for professional development for staff, such as the UTQ course. The panel appreciates that staff is very accessible to students and is highly committed to the programme. The panel notes that the workload is heavily concentrated on two core teachers, which may not be sustainable in the long term. While the panel acknowledges that improvements have already been made and the intention to hire an Educational Technical Coordinator (ETC) to alleviate this burden is commendable, the panel recommends monitoring workload distribution to ensure it remains manageable for all staff, and finalize the hiring of an ETC as soon as possible to provide much-needed support. Since the current technical coordinator is leaving, the recent replacement of the technical coordinator is a positive step, particularly if the programme succeeds in attracting a candidate who can commit long-term. Offering a clear career path for this role would further strengthen organizational stability and improve the quality of support for students and faculty.

Considerations

The curriculum is well aligned with the intended learning outcomes, employing a variety of teaching methods that are effective to achieve these goals. The programme is distinguished by its practical, hands-on approach, featuring numerous projects that allow students to explore their own interests, and an ambitious range of topics and skills covered in the curriculum. The panel advises the programme to annually review and include emerging topics in courses, while continuously monitoring developments in security and network engineering, and making strategic choices in collaboration with the Professional Advisory Board to adapt curriculum content as needed. The panel appreciates the opportunity for students to study part-time, which reflects the programme's student-centered approach and enhances its appeal to working professionals. It recommends exploring more flexible arrangements for part-time students to complete the 3-month research project, and that any changes be clearly communicated to part-time students. Teaching the programme in English is appropriate and fully supports the rationale for using English as the language of instruction and in the programme name. The panel concludes that the admission requirements are appropriate and the curriculum is feasible. The panel is very positive about the strong commitment that the programme demonstrates to fostering a welcoming and inclusive environment for students, and the highly qualified and committed teaching staff. The panel recommends monitoring staff workload distribution to ensure it remains manageable for all staff.

Conclusion

The panel concludes that the programme meets standard 2.

Standard 3. Student assessment

The programme has an adequate system of student assessment in place.

Findings

System of assessment

The assessment and examination policy is documented in the Teaching and Examination Regulations (TER), which contain both programme-specific regulations and general faculty-wide regulations such as examination rules, retake rules and the right of inspection by students. Examination and assessment adhere to UvA assessment policy (Kader Toetsbeleid, University of Amsterdam, 2022), complemented on institute level by the GSI Assessment Plan (Toetsplan). The GSI Assessment Plan informs examiners and students about all rules governing assessments, including types of assessments, and aims to ensure the quality, validity, and fairness of examinations. Furthermore, exams are organized according to a faculty-wide invigilation protocol.

All courses contain multiple assessments, and throughout the programme a diverse palette of examination techniques is used, from written exams to essays, reports, presentations, to lab work. Most courses feature individual assessment to prevent students passing solely based on group work. Within most assessment, the focus is on either competence or insight, whereas assessment purely based on knowledge is rare. Assessment consists mostly of formative tests, stimulating students to proactively learn and reflect and making use of feedback from fellow students and staff to improve. Most examinations are not only graded, but also extensively discussed with the student. The programme uses an automatic plagiarism check, which is facilitated by the Canvas platform. For each course, a dedicated examiner is appointed by the Examinations Board upon recommendation by the programme director. Usually, the examiner coincides with the course coordinator. According to FNWI policy an examiner should at least be UD-level with a permanent contract and BKO qualification.

Regarding the role of GenAI, the programme acknowledges the transformative potential of this technology in education while being mindful of the associated risks. The UvA has developed a policy framework guiding the deliberate and thoughtful integration of AI tools in education, and the Faculty of Science is actively developing faculty-specific policies. One of the faculty members has started a Senior Teaching Qualification (STQ; Senior Kwalificatie Onderwijs - SKO) project focused on the integration of GenAI in the programme, exploring how to incorporate GenAI tools responsibly and effectively in assessments and learning activities. The panel came to understand that the UvA and the Faculty of Science have had a conservative approach toward GenAI in education. Recent developments show a more proactive stance, including pilot projects, policy frameworks, and the rollout of GenAI services such as the UvA Chat. The programme is engaging with the challenges and opportunities posed by generative AI in assessment through updating assessment policies and guidelines and through researching assessment implications. This reflects an understanding that the programme must adapt its assessment practices to maintain validity and reliability in the context of emerging AI technologies. The panel encourages the programme to continue working on clear and uniform procedures to address the use of GenAI.

The panel is positive about the assessment system in the master's programme SNE, and finds that the quality of the assessment and quality assurance process is up to standard. The programme ensures transparency amongst others by applying the four-eyes principle. Assessment methods are varied; the panel especially appreciates the attention paid to individual assessment functioning next to group-based assessment.

Examination Board

The Examination Board (EC) is part of the Examination Board Exacte Wetenschappen/ Informatiewetenschappen, which is one of two Examination Boards at faculty level. Daily routine is handled by a subcommittee for the programmes MSc Software Engineering and MSc Security and Network Engineering. The EC appoints examiners for all courses as well as for the supervision of graduation projects. The EC also makes decisions regarding all non-standard requests, such as exemptions or additional examination opportunities, as well as student complaints that could not be otherwise resolved. The EC takes action concerning plagiarism and fraud. For that cause, the EC has installed a corresponding subcommittee that handles cases of plagiarism and fraud in a programme independent way. Moreover, the EC investigates an annual sample of graduation projects and individual courses, assessing both the quality of the thesis or course in general and adherence of student assessment to the various regulations in particular. Lastly, the EC advises the programme director and the course coordinators in all assessment related matters, among others the Teaching and Examination Regulations (TER).

Based on the documentation and discussions during the site visit, the panel concludes that the EC functions quite well and fulfils all of its legal duties in a responsible and satisfactory way, and is in control of assessment quality with the use of sampling of courses and graduation projects. The quality mechanisms allow the Board to monitor course assessment quality in the programme and exit level of students. The panel notes that the programme could benefit from the joint EC with the MSc Software Engineering to align assessment practices even more, also with regard to the 3-month research project, to avoid having to find out all by themselves.

Graduation project assessment

The 3-month graduation project is assessed by a defence committee that consists of the academic supervisor, if applicable the daily supervisor(s) from either industry or academia, and an independent second reader. Every graduation project is finalized with a defence, which contains a 20 to 25-minute presentation of the student, followed by questions from the defence committee and the general audience, where students defend their project in a scientific discourse. Following the public defence, the defence committee withdraws for deliberation. The deliberation is organized around three subjects that are independently assessed: the research itself (daily and academic supervisors) counts for 40% of the final grade, the written thesis (whole committee) counts for 40% and the oral presentation and scientific discourse (whole committee) counts for the remaining 20%. A student must receive a passing grade in each sub-component to pass the graduation project, which typically is the last remaining curriculum component for graduation. During deliberation, the defence committee will make use of an online evaluation form in the DataNose platform to document the assessment of the committee in detail and clearly motivates the final overall grade. Grading is done by the two examiners: the academic supervisor and the second reader. The daily supervisor, either internal or external, only has an advisory role. At last, the academic supervisor and second reader convey the outcome of the defence to the student, including the motivation for the grade.

The examiners of the graduation project are put forward by the programme director and are appointed by the Examinations Board. Responsibility for supervision can be partly delegated to a post-doctoral researcher or PhD candidate. However, the final quality check is performed by the examiner. The second reader is ideally an examiner from a related area of expertise, who is not directly involved in the project. The second reader independently assesses and grades the thesis and the final presentation of the graduation project. The examiners make use of a thesis assessment rubric, to ensure transparency and consistency of the grading process.

The panel examined the thesis assessment procedures and a sample of 15 completed assessment forms prior to the site visit. It concludes that the assessment of the thesis is up to standard, and appreciates the clear attention, care and thoroughness that is paid to evaluating final projects. The four-eyes principle is consistently applied, requiring the involvement of at least one formal examiner, which adds to the validity of the assessment. The panel also values that the graduation project assessment includes an oral defence, which is useful in the light of generative AI and adds to the active learning process of students.

The panel notes that the current process does not have a structured intermediate evaluation moment to monitor student progress and provide timely feedback. Although the programme asks students to give short presentations during the graduation project process, these do not yet include formal, prefixed evaluation points to determine whether students are on track or need to adjust their approach. The panel advises introducing formal intermediate evaluation dates during the graduation project, to assess student progress and identify necessary adjustments.

Considerations

The system of assessment in the master Security and Network Engineering is reliable, valid and transparent. Assessment methods are varied, and checks and balances are in place to ensure course and graduation project assessment quality. The Board of Examiners is in control and fulfils all of its legal duties in a satisfactory way. Graduation project assessment is up to standard, with the consistent use of a four-eye principle in grading and the use of an thesis assessment rubric to substantiate the grades. The panel values the oral defence as substantial part of graduation project assessment, which in the opinion of the panel is useful in the light of generative AI and adds to the active learning process of students. The panel advises introducing formal intermediate evaluation dates during the graduation project process to assess student progress.

Conclusion

The panel concludes that the programme meets standard 3.

Standard 4. Achieved learning outcomes

The programme demonstrates that the intended learning outcomes are achieved.

Findings

Graduation projects

In preparation of the site visit, the panel studied a selection of 15 recent master's theses. It found all graduation projects theses to be up to standard, and the works demonstrated solid research skills. Most research projects are performed in external organizations, in line with the aim of the programme. The panel also noted with appreciation that many master theses have led to scientific publications, which is also encouraged by programme management. The panel considers the quality of the final products to be convincing proof of the realization of the intended learning outcomes by graduates.

Alumni

A recent alumni survey (2025) and exit evaluation data show that graduates generally are satisfied with the programme and the acquired knowledge and skills. They feel well prepared for the professional field, and graduates are in a good position to find a job. Most graduates find a job in industry. Many graduates who completed their graduation project in industry are offered a position by the host company. Not all accept this offer as they usually have the choice between multiple attractive positions.

Considerations

The quality of the graduation projects and the performance of graduates show that students of the MSc Security and Network Engineering realize the programme's intended learning outcomes. The graduation projects, many of which have resulted in academic papers, demonstrate solid research skills and suitably reflect the cybersecurity and networking profile of the programme.

Conclusion

The panel concludes that the programme meets standard 4.

General conclusion

The panel judges that the master's programme meets all four standards. The panel's assessment of the programme is therefore positive.

Recommendations

1. Explore more flexible arrangements for part-time students to complete the 3-month research project in combination with their professional commitments, and communicate changes clearly to student.
2. Monitor workload distribution to ensure it remains manageable for all staff.

Appendix 1. Intended learning outcomes

1. The student has knowledge of network protocols & software, of operation of networks and of innovative networking technologies.
2. The student has knowledge of security challenges of systems on all levels, including networks, software and hardware.
3. The student can evaluate network protocols, software and technologies & engineer concrete network systems.
4. The student can evaluate the security of systems and engineer concrete solutions that eliminate real-world security problems.
5. The student can critically analyse, evaluate and synthesise the ethical aspects of their research.
6. The student can communicate their work and results to a specialist and non-specialist audience.
7. The student can autonomously conduct research and can contribute to open science.

Appendix 2. Programme curriculum

MSc Security and Network Engineering 2025-2026 - fulltime									
Period 1		Period 2		Period 3	Period 4		Period 5		Period 6
September	October	November	December	January	February	March	April	May	June
Security of Systems and Networks (6EC)		CyberCrime and Forensics (6EC)		Offensive Technologies (6EC)		Advanced Security (6EC)		Research Project (18EC)	
InterNetworking and Routing (6EC)		Large Systems (6EC)				Advanced Networking (6EC)			

MSc Security and Network Engineering 2025-2026 - part-time year 1										
Period 1		Period 2		Period 3		Period 4		Period 5		Period 6
September	October	November	December	January		February	March	April	May	June
Security of Systems and Networks (6EC)		CyberCrime and Forensics (6EC)		Offensive Technologies (6EC)		Advanced Security (6EC)				
MSc Security and Network Engineering 2025-2026 - part-time year 2										
Period 1		Period 2		Period 3		Period 4		Period 5		Period 6
September	October	November	December	January		February	March	April	May	June
InterNetworking and Routing (6EC)		Large Systems (6EC)				Advanced Networking (6EC)		Research Project (18EC)		

Appendix 3. Programme of the site visit

08.45-09.15	Welcome and panel preparation
09.15-10.00	Interview programme management
10.00-10.15	Internal panel session/break
10.15-11.00	Examinations Board & Programme Committee
11.00-11.15	Internal panel session/break
11.15-12.00	Interview MSc students and alumni
12.00-13.00	Lunch
13.00-13.45	Interview MSc SNE staff
13.45-14.00	Internal panel session/break
14.00-15.00	Thematic Session
15.00-15.45	Internal panel session
15.45-16.30	Concluding session programme management
16.30-17.15	Concluding internal panel session
17.15-17.45	Public feedback from the panel followed by a reception

Appendix 4. Materials

Prior to the site visit, the panel studied 15 theses. Information on the theses is available from Academion upon request.

The panel also studied other materials, which included:

- SNE Reading Guide 2026
- SNE Teaching and Examination Regulations
- SNE Exit Qualifications
- SNE partners survey results
- Minutes Professional Advisory Board
- Procedure UvA SNE admission
- SNE welcome session slides 2025
- PAB meetings in PAB minutes
- Visible Learning Trajectories
- Course materials of Advanced InterNetworking and Routing (INR), Offensive Technologies (OT) and Advanced Networks (AN)
- List of graduation projects
- List of External Research Projects
- SNE Research Project Supervisor List
- List of external teaching staff – guest lecturers
- FTE Allocation Table
- Human Capital Agenda Security
- National Cyber Security Research Agenda IV
- Cybersecurity workforce study 2023 and 2024
- Kader toetsbeleid
- Assessment plan
- Thesis assessment rubric
- Proposal SAEQ – Examinations Board
- Yearly report Programme Committee 23-24
- Yearly report Examinations Board 23-24
- Exam Board Assessment 2025
- UvA GenAI policy
- Outcome Alumni Questionnaire
- NSE results 2021-2024