NVAO

PROGRAMME ASSESSMENT

Lycée Guillaume Kroll
BTS Cybersecurity

Final report submitted to the Ministry of Research and Higher
Education on 28 January 2026

Programme Assessment

LYCÉE GUILLAUME KROLL

BTS CYBERSECURITY

Final report submitted to the Ministry of Research and Higher Education on 28 January 2026

Content

4 | Lycée Guillaume Kroll – BTS Cybersecurity
    □ November 2025
    NVAO □ Confidence in Quality

1 Executive Summary

This document reports on the programme assessment of the 'BTS Cybersecurity' programme at the Lycée Guillaume Kroll (LGK) by an international expert panel convened by NVAO on behalf of the Ministry of Research and Higher Education of Luxembourg.

The programme was accredited by the Luxembourg authorities following an assessment in 2021. The current panel studied the self-evaluation report submitted by the Lycée Guillaume Kroll and discussed the state of play of the programme with a variety of stakeholders on November 13rd, 2025.

The panel praised LGK for the clear professional orientation and well-defined objectives of the BTS Cybersecurity programme. The programme is strongly practice-based and aligned with EQF level 5, aiming to prepare students for operational roles in cybersecurity within a two-year timeframe. It combines solid technical foundations with transversal skills, supporting adaptability in a fast-evolving digital sector. Strong links with industry, including applied projects, internships, and frequent external interventions, ensure close alignment with labour-market needs. Employers and alumni confirm the programme's high relevance and employability, while opportunities to continue into bachelor studies further enhance its academic and professional value. The panel further underlined the staff's high level of commitment, accessibility, and effective collaboration.

Building on these strengths, the panel has formulated a set of targeted recommendations aimed at further enhancing the programme's pedagogical effectiveness, student guidance, organisational resilience, and quality assurance processes.

- Assessment area 1: **Introduce post-session debriefings for highly technical external expert interventions** to maximize pedagogical impact.
- Assessment area 1: **Enhance guidance on progression to Bachelor programmes by providing** more accessible information and structured support to help students navigate these pathways.
- Assessment area 2: **Further strengthen the visibility and promotion of the BTS** to attract a wider and more diverse pool of prospective candidates and to enhance awareness of the programme.
- Assessment area 3: **Strengthen team resilience** by reducing dependency on key individuals through improved internal knowledge sharing, documentation of practices, and mentoring within the teaching team.
- Assessment area 4: **Adopt more systematic approaches to analysing and documenting student and employer feedback**, ensuring that curricular updates and strategic decisions are clearly recorded and followed up.

Following the comprehensive investigation into the quality of the BTS Cybersecurity, the panel concludes that the programme meets all assessment areas.

Consequently, the panel recommends a re-accreditation.

Assessment area		Judgement
1	Aims and objectives of the study programme	MET
2	Admission, evaluation, certification	MET
3	Implementation of the programme	MET
4	Quality assurance measures	MET
	Overall judgement	**Re-accreditation advice**

The Hague, December 2025

On behalf of the international expert panel charged with the programme assessment of the Lycée Guillaume Kroll - BTS Cybersecurity,

Nicolas Navet   Gwenny Nurtantio

Chair   Secretary

2 Introduction

The Ministry of Research and Higher Education of Luxembourg (MESR) requested the Accreditation Organisation of the Netherlands and Flanders (NVAO) to carry out a programme assessment of the BTS Cybersecurity (BTS) offered by Lycée Guillaume Kroll (LGK). The programme was accredited for the first time in 2021. The present assessment report serves as an advisory document to MESR, which will ultimately decide on the reaccreditation of the BTS Cybersecurity offered by Lycée Guillaume Kroll.

In view of the specific nature of this request, the NVAO convened an international panel of experts consisting of:

- Mr Nicolas Navet, Luxembourg, chair;
- Mr Yoann Klein, Belgium, member;
- Ms Ann Das, Belgium, member;
- Mr Koen De Bruyne, Belgium, student-member.

The composition of the panel reflects the expertise deemed necessary by NVAO for this accreditation exercise. Short CVs of the panel members are provided in annex 1 (5.1). On behalf of NVAO, Mr David Corradi was responsible for the coordination of the assessment process. The external secretary, Ms Gwenny Nurtantio, drafted this report in close cooperation with all panel members and in agreement with the chair. All panel members and the secretary signed a statement of independence and confidentiality.

The panel carried out the assessment after which the Board of NVAO made a recommendation to the Ministry. The Ministry takes the final accreditation decision. The framework for assessment comprises the criteria under the Higher Education Law of 21 July 2023, which creates the legal basis for the short-cycle programmes leading to the Brevet de Technicien Supérieur (BTS), offered by the Lycées.

The panel members studied the self-evaluation report and submitted their first impressions on the materials prior to the preparatory panel meeting, which was held online on November 10th, 2025. The site visit took place on November 13rd, 2025. The panel talked to the management of the Lycée Guillaume Kroll and the programme, as well as to teaching staff, students, alumni and representatives of the professional field. The panel was also given a guided tour of the lycée, allowing members to observe facilities, learning environments, and practical teaching arrangements in use. The schedule of the visit is presented in annex 2 (5.2). Annex 3 (5.3) lists the materials made available by the programme before the site visit.

Immediately after the discussion, the panel formulated its considerations and preliminary conclusions. These are based on the findings of the site visit and build on the assessment of the documents. The external secretary then drafted the advisory report and circulated it to all panel members for review and feedback. The comments of the panel were incorporated in a second version, which was validated by the chair and submitted to the Lycée Guillaume Kroll for comments on factual errors. The Ministry of Research and Higher Education in Luxembourg also received the report for a factual error check. Following this review, a final

7   Lycée Guillaume Kroll – BTS Cybersecurity
     □ November 2025
     NVAO □ Confidence in Quality

draft was prepared and submitted on behalf of the panel to NVAO, which in turn will send the report to the Ministry of Research and Higher Education in Luxembourg.

3 Programme assessment BTS Cybersecurity

3.1 Assessment area 1: Aims and objectives of the programme

Assessment area 1 is detailed in the following assessment criteria:

a) The programme complies with the provisions relating to programmes leading to the BTS, as defined in Title II[1].
b) The programme has a **coherent curriculum** which reflects the programme's intended l**earning objectives** and the **learning outcomes** to be achieved by the student. It is broken down into **knowledge, specific skills, and transversal skills**.
c) The programme is defined in accordance with **European standards** and the Bologna Process. It is defined in terms of **ECTS credits**.
d) The programme is **divided into modules**, each of which is awarded a certain number of ECTS credits. Each module is made up of one or more theoretical or practical units, known as "**courses**". Each course carries a minimum of one ECTS credit and a maximum of 20 ECTS credits. The objectives and learning outcomes of each module and course are clearly defined.
e) The **workload** is appropriate and balanced between semesters.
f) The **ratio of theoretical to practical teaching** is consistent with the programme's objectives.
g) **For each module** of the programme, the appropriateness of the **workload**, the types and methods of **assessment** and the intended **learning outcomes** are determined and documented in relation to the **level 5** descriptors of the Luxembourg Qualifications Framework, in accordance with the amended Law of 28 October 2016 on the recognition of professional qualifications[2] [3], and in relation to the number of ECTS credits allocated to each module of the programme.
h) Programmes preparing for **regulated professions** within the meaning of the amended Act of 28 October 2016[4] on the recognition of professional qualifications **comply with the legislative and regulatory requirements governing the regulated profession concerned.** This compliance is established by means of a detailed **report drawn up by the competent minister responsible** for the profession concerned. This report is a **mandatory part** of the accreditation file.

The BTS Cybersecurity curriculum is a practical and technical programme delivered over four semesters, leading to a short-cycle **higher education diploma of 120 ECTS**. The programme equips students with both hard and soft skills to manage complex operational tasks, including risk assessment, regulatory compliance, and system and network protection, while fostering adaptability to emerging technologies. The panel praised the ambitious learning objectives, noting that students acquire competencies consistent with **Level 5 expectations**, including autonomy, problem-solving, and professional responsibility. Employers confirm that graduates have a solid technical foundation, are versatile, and can integrate directly into operational teams. The panel observes that some learning outcomes are positioned slightly above Level 5. This is, however, justified in the given context, as they align well with current industry demands and the programme demonstrates its capacity to deliver these outcomes effectively, without this leading to student failure.

---

[1] https://legilux.public.lu/eli/etat/leg/loi/2023/07/21/a470/jo#title_2

[2] https://legilux.public.lu/eli/etat/leg/loi/2016/10/28/n2/jo

[3] https://legilux.public.lu/eli/etat/leg/loi/2016/10/28/n2/jo#art_69

[4] https://legilux.public.lu/eli/etat/leg/loi/2016/10/28/n2/jo

Semesters 1 to 3 combine foundational and applied cybersecurity knowledge with programming, AI, project management, communication, and professional autonomy, delivered through a balanced mix of directed instruction and guided independent work. The workload is structured to ensure progressive learning, and students find it well-balanced, allowing time for personal projects, exploration, and research. The panel highlighted that students successfully **balance the acquisition of theoretical knowledge with its practical application**, applying knowledge directly to projects and exercises. Students appreciate the hands-on approach and the opportunity to explore advanced topics through **interventions by external experts**, which introduce current trends and technologies in areas like blockchain, AI, and cybersecurity. The programme's flexibility, which allows content to adapt to emerging technologies and market trends, was highlighted as a major strength. **The panel recommended adopting a more systematic approach to integrating these emerging technologies throughout the curriculum**, ensuring they are consistently covered across all modules. Furthermore, the panel also recommended providing additional debriefing time after highly technical external interventions to ensure pedagogical clarity and reinforce learning outcomes.

Semester 4 is fully dedicated to professional immersion, comprising the completion of a final project supervised by an academic promoter and a **12-week full-time internship**. The panel praised the strong **connection with the labour market**, highlighting the programme's alignment with employer expectations and its contribution to high employability. Alumni emphasised that the programme offers a broad and practical perspective, allowing graduates to understand multiple domains and tools, which positions them as immediately operational in cybersecurity roles.
Students value the opportunity to continue into bachelor programmes, and the panel suggested offering additional guidance and support to help students navigate these transitions effectively.

The panel also noted the programme benefits from extensive engagement with **external experts and industry partners**, including participation in events such as Hack.lu, Cyber Fortress, and Cybersecurity Days, which enrich learning and strengthen professional connections. Students particularly appreciated these interventions, which expose them to real-world applications and current trends in cybersecurity. To maintain consistency with Level 5 expectations, **the panel recommended strengthening the onboarding process for external lecturers**, ensuring they are fully informed about learning objectives and expected outcomes, while preserving the programme's practical and adaptive approach.

Conclusion
The panel concludes that the BTS Cybersecurity programme at the Lycée Guillaume Kroll meets **Assessment Area 1**. This two-year programme (120 ECTS) combines theoretical instruction with a 12-week full-time internship and a final project, providing a coherent curriculum that develops technical and professional skills while fostering autonomy and initiative. Graduates are well-prepared for employment in operational cybersecurity roles and for further studies.

The programme is well aligned with labour-market needs, and employers confirm that graduates are technically proficient, adaptable, and immediately operational. The panel praised the ambitious learning objectives, practical orientation, and strong engagement with external experts and industry events.

To further enhance alignment with EQF Level 5, the panel recommended strengthening the onboarding of external lecturers, providing additional debriefing after highly technical interventions, maintaining a systematic approach to keeping the curriculum aligned with evolving technologies, and offering guidance for students pursuing bachelor programmes,

Overall, the BTS Cybersecurity provides a robust, adaptive, and industry-relevant education that effectively prepares students for professional and academic pathways.

3.2   Assessment area 2: Admission, evaluation, certification

Assessment area 2 is detailed in the following assessment criteria:

a) **The Lycée publishes**, in a clear, precise, and up-to-date manner, i**nformation on its BTS programmes**, the **respective status** of its programmes with regard to accreditation, the **admission requirements** for the various programmes, **the enrolment fees**, the **total cost** to be expected per programme, **the curriculum** for the programmes offered, the **intended learning outcomes** and the **qualifications** leading to said programmes.

b) The **admission requirements** for the programme of study are clearly defined and published. The modalities of potential **entry examinations** must be published 3 months in advance.

c) The procedure for the **validation of prior learning or experience** are clearly defined, in accordance with the provisions of Article 11[5].

d) **Assessment methods** are defined in relation to the learning objectives and are designed to verify the achievement of the programme's intended learning outcomes.

e) **The assessment methods** applied in the various modules and courses are clearly **communicated** to the students.

f) **The degree shall comply with the provisions** of Article 26(2)[6], and shall be **accompanied by a supplement** complying with the provisions of Article 26(3)[7].

Admission

Information on the BTS Cybersecurity programme is available on the LGK website (www.lgk.lu/cyb) and the LMS platform, where prospective students can find comprehensive details about the programme's objectives, course catalogue (modules, descriptions, competencies, assessment and teaching methods), career opportunities, accreditation status, admission requirements, registration fees, and internship procedures. Organisational details, including exam dates, internship documents, tutor assignments, and scholarship information, are also provided via the LMS (eduMoodle36), managed by the Centre de Gestion Informatique de l'Éducation (CGIE).

The admission process starts in mid-April through the guichet.lu portal or the dedicated website https://enroll-bts.lgk.lu. Candidates must submit an online application with the necessary documents by the end of June. For applicants with Luxembourgish technician diplomas who have not completed preparatory modules, a preliminary access test is required. The admission includes a practical test based on course content and an interview to evaluate candidates' motivation and proficiency in French and English. The selection process is competitive, and candidates are ranked, with the top applicants being admitted after validation by the ad-hoc admission committee, chaired by a Ministry representative.

The programme offers a clear procedure for **validating prior experience (VAE),** with a dedicated commission consisting of the programme director, two teaching staff members, and two industry professionals. While no VAE requests have yet been submitted, the process is defined and accessible.

---

[5] https://legilux.public.lu/eli/etat/leg/loi/2023/07/21/a470/jo#art_11

[6] https://legilux.public.lu/eli/etat/leg/loi/2023/07/21/a470/jo#art_26

[7] https://legilux.public.lu/eli/etat/leg/loi/2023/07/21/a470/jo#art_26

The panel commended the clear communication of the admission requirements, including pre-requisites, tests, and procedures. They also noted that while the programme is selective, it is not overly restrictive, allowing for the inclusion of motivated and capable students. Feedback from students indicates that they find the admission test manageable, particularly for those with IT backgrounds.

The panel recommended continuing to enhance the visibility of the programme by strengthening outreach and promotional activities and by exploring additional channels and media to reach a wider pool of prospective students. The panel also encourages the programme to reflect on targeted communication strategies aimed at increasing the attractiveness of the curriculum for women.

The panel notes that the current limit of 14 students ensures individualised supervision and excellent learning outcomes but also limits the programme's ability to meet the growing demand on the labour market. The panel therefore encourages the institution to reflect strategically on future capacity—considering when and under which conditions an increase in student number could be envisaged—while maintaining the high quality and personal approach that currently distinguish the programme.

Evaluation

Assessment methods for the BTS Cybersecurity programme are clearly defined in each course syllabus and communicated to students at the start of the semester via the catalogue and the LMS (eduMoodle). They include continuous assessment, written, oral, and practical examinations, individual and group work, reports, personal projects, lab exercises, internships, and the final project.

The programme complies with the legal framework defined in the Law of 21 July 2023 on higher education (Chapter III, Articles 13 and 14), including rules for assessment, validation, and examination committees. Dates and modalities for all assessments are communicated via the academic calendar, with continuous assessment monitored by instructors and formal examinations coordinated by the programme coordinator.
Formative assessments are used where appropriate, and the coordinator ensures alignment with programme objectives, consistency across teachers, and adherence to published evaluation criteria. Students generally report satisfaction with the clarity and fairness of assessment methods, and alumni confirm that evaluations prepare them well for practical and professional cybersecurity tasks.

The panel notes that evaluation practices are transparent, coherent, and aligned with Level 5 expectations.

Certification

The diploma and supplement are compliant with Luxembourgish law.

The panel highlights the low dropout rate, attributing it to the quality of recruitment, student motivation, and the supportive academic framework.

Conclusion

The panel concludes that the BTS Cybersecurity at the LGK meets Assessment Area 2. The programme demonstrates clear, fair, and coherent admission and evaluation processes. The selective yet accessible admission ensures motivated and capable students, while assessment methods effectively support learning, professional skills, and Level 5 competencies. The low dropout rate reflects the programme's strong recruitment, student engagement, and supportive academic environment.

3.3 Assessment area 3: Implementation of the programme

Assessment area 3 is detailed in the following assessment criteria:

> a) The programme **has sufficient resources in terms of teaching staff and financial and material means** to meet its specific needs and achieve its objectives. These resources are available throughout the entire duration of the programme.
> b) The Lycée has **appropriate infrastructure** to offer the proposed programme and enable its students to do achieve the intended learning outcomes.
> c) Teaching is provided by a **teaching staff that is competent** from a didactic and pedagogical point of view and capable of relating teaching to professional practice in the field concerned and to current research. Teaching is student-centred and encourages active student participation. The suitability of each of the professional profiles of the available and planned teaching staff is clearly demonstrated in relation to the programme's objectives and its intended learning outcomes.
> d) The **proportion between teachers appointed in the Lycée and external contractors** is appropriate to the objectives of the curriculum, it being understood that the **proportion of lessons provided by external contractors may not exceed the threshold of 40% set in Article 9(2)[8].**
> e) **Continuing training programmes** are provided for teaching staff.
> f) In the case of alternate programmes, the school has a specific and compulsory **training programme for the trainers who deliver the practical teaching modules in the workplace**.
> g) Students benefit from appropriate supervision and full information. A **tutoring programme** is offered to students.

The BTS Cybersecurity programme is delivered primarily by internal teaching staff with substantial professional experience, complemented by **external experts** for emerging topics. The proportion of external teaching **does not exceed 40%** of total lessons, in compliance with Article 9(2) of the Law of 21 July 2023. Internal staff demonstrate strong engagement, motivation, and pedagogical competence, having undergone formal training in active and student-centred teaching methods. They maintain up-to-date knowledge through continuous professional development, regular participation in workshops, conferences, and industry events.

Teaching is structured to balance theoretical and practical learning, with morning sessions dedicated to formal courses and afternoons often reserved for external interventions. Practical work is a major component of the curriculum, representing approximately 70% of the programme, and is delivered in small groups to ensure close supervision. Students benefit from a learning-by-doing approach, cooperative pedagogy, and discovery-based methods that encourage autonomy, critical thinking, and direct application of theory to professional contexts.

Regular coordination occurs both formally, through curricular group meetings, and informally, through daily interactions among staff. Decisions on course content, teaching methods, and adjustments based on student or professional feedback are discussed within the teaching team. The programme also integrates technological updates, ethical

---

[8] https://legilux.public.lu/eli/etat/leg/loi/2023/07/21/a470/jo#art_9

considerations, and emerging practices, such as AI and quantum computing, ensuring content remains current and relevant to industry needs.

The Lycée provides dedicated **facilities** for the BTS Cybersecurity programme, including two classrooms reserved for first and second-year students. The IT infrastructure supports a realistic, secure, and isolated simulation environment. A dedicated network ("playground") allows for high-risk exercises such as penetration testing, DoS attacks, intrusion detection, and incident response without compromising production or sensitive systems. The panel considers these facilities to be appropriate for the current size of the programme, while noting that an expansion of dedicated classroom capacity would be necessary should the programme grow further.

The practical environment includes a suite of servers simulating a typical corporate infrastructure, with firewall, DHCP, DNS, mail, web, SIEM, Docker hosts, and RADIUS servers, managed by instructors. A virtualisation platform (Proxmox VE) and a "cyber range" environment provide students with hands-on access to realistic simulations. Additional equipment, including mobile network racks and professional-grade hardware, is maintained internally or supplied by partner organisations. The infrastructure meets current needs, with plans for extension by 2030 to accommodate programme growth.
Students receive structured individual **tutoring** throughout the programme. Each student is assigned a tutor at the start of the first semester, who provides regular meetings (at least once per semester) and additional support as needed. Tutors guide students on academic progress, projects, internships, and career planning. Reports are produced after each meeting to ensure continuity. The Service psycho-social et d'accompagnement scolaires (SePAS) provides confidential personal support to students facing challenges, enhancing engagement and academic success.

Information is communicated transparently via a Learning Management System (eduMoodle), Microsoft Teams, Outlook calendars, and email, providing students with real-time access to schedules, documents, and resources. Tools and approaches mirror professional standards, preparing students for the transition to the workplace.

The panel notes that the programme actively engages with the **professional cybersecurity sector**. Students participate in events such as Cybersecurity Days, conferences, and networking sessions. External speakers provide practical insights, career advice, and guidance on emerging technologies. Project work and evaluations incorporate both technical and managerial skills, with feedback from instructors and industry professionals ensuring relevance and quality. Alumni report that this combination of theory, practice, and professional exposure supports rapid integration into the workforce. All **teaching staff** undertake ongoing **professional development**. Over 800 hours of continuous training have been recorded, ensuring that competencies remain current and aligned with the rapid evolution of cybersecurity. Teachers regularly complete more training hours than required, demonstrating a strong commitment to teaching and keeping their professional skills up to date.

Conclusion

The panel finds that the programme meets the assessment criteria for area 3. The BTS Cybersecurity programme benefits from highly qualified and motivated teaching staff, robust infrastructure, and extensive student support mechanisms. The combination of theoretical instruction, hands-on practice, and strong industry integration creates a high-quality and comprehensive learning environment. While the programme's current resources are sufficient, **the panel encourages ongoing reflection on sustainability, particularly regarding staff workload and future expansion plans.**

3.4 Assessment area 4: Quality assurance measures

Assessment area 4 is detailed in the following assessment criteria:

> a) **The Lycée ensures the collection, analysis, and use of relevant information for the effective management and continuous improvement of its BTS programmes**.
> b) The Lycée has a **quality assurance system** for its BTS programmes, which it makes **publicly available**. The quality assurance procedures applied by the Lycée **comply with** the requirements of the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG).
> c) **The programmes are regularly subjected to internal evaluation to ensure that they take into account the latest research and didactic developments in the relevant field,** achieve the intended learning outcomes, and **meet the constantly evolving needs of students and society**.
> d) The Lycée maintains regular and formalised **exchanges with professional circles in the Grand Duchy of Luxembourg** related to its BTS programmes.
> e) **Responsibilities, competencies, and decision-making processes related to the BTS programme** are **defined clearly and transparently.**
> f) **Teachers and students** have sufficient means to express their positions and **participate** in decision-making through representation in various bodies and committees.
> g) In the case of an application for the **reaccreditation** of a programme, it is demonstrated to what extent, and through which means, actions, and decisions **the Lycée has taken into account the recommendations outlined** in the evaluation report and the accreditation decision of the previous period.

The Lycée Guillaume Kroll has established a systematic approach to **collect, analyse, and utilise information from multiple stakeholders** to ensure the effective management and continuous improvement of its BTS programmes. Student **feedback** is gathered through semester-end questionnaires assessing course content, teaching quality, and resource availability. Inputs from student internships and projects provide practical insights into the alignment of the programme with professional requirements. In addition, teachers and external experts contribute through formal and informal exchanges, allowing for the ongoing adjustment of course content and methods to reflect emerging industry trends, technological developments, and regulatory changes. These measures create a robust framework for data-driven programme management.

The Lycée operates a quality assurance system that is **publicly accessible** and fully compliant with the **Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG).** The system encompasses internal evaluations, annual reviews, and formal re-accreditation processes with the NVAO. Procedures include course design, approval, delivery, and assessment, as well as recruitment, training, and development of teaching staff. Key documents, such as programme regulations and evaluation results, are communicated transparently to all stakeholders.

BTS programmes undergo continuous **internal evaluation** to ensure alignment with the latest research, pedagogical developments, and evolving societal and student needs. The curriculum is regularly reviewed by the programme group, which integrates feedback from students, teachers, and industry representatives. Adjustments have included course content updates, restructuring of modules, and the incorporation of practical exercises. Evaluation extends to

student performance, internship outcomes, and professional insertion, ensuring that learning objectives are achieved and remain relevant to the job market.

The Lycée maintains structured and informal interactions with the **professional community in Luxembourg.** External experts from industry and governmental institutions are invited to contribute to courses, workshops, and networking events. Student internships are closely monitored through joint supervision by professional and school-based tutors, enabling feedback on skill development and curriculum relevance. The creation of the "Amicale des BTS du LGK asbl" further strengthens these ties by organizing annual networking events, technical visits, and alumni engagement initiatives. This active collaboration ensures that the programme remains closely linked to the skills and competencies demanded in the labour market.

However, much of this cooperation still relies on informal contacts and individual initiatives. To ensure consistency and sustainability, **the panel recommends adopting a simple and pragmatic approach to the collection, documentation, and review of industry feedback**. Such an approach would help maintain the programme's flexibility and quality while reducing dependence on individual actors.

Roles and responsibilities within the BTS programmes are clearly defined and communicated. Teachers are responsible for implementing course content and evaluating student performance. Students actively participate in learning and provide feedback to inform programme improvements. The director ensures that necessary resources are available, while the coordinator oversees programme implementation and alignment with regulations. The curricular group defines learning objectives, updates content, and makes decisions regarding programme modifications, which are validated by the Ministry of Higher Education. Decision-making processes are transparent, documented, and communicated to all stakeholders.

Both teachers and students have **multiple channels to express their views** and participate in programme-related decisions. Students provide feedback through questionnaires and tutor meetings, while teachers engage in formal and informal discussions with coordinators and peers. Although there is currently no formal student representation, the small class sizes and frequent interactions allow for active participation and rapid incorporation of feedback. External stakeholders, including employers, contribute through advisory sessions, internships, and course interventions.

To enhance this collaborative model, and in line with the earlier observation regarding industry engagement, the panel encourages the introduction of more formalized processes to gather and track employer feedback regularly, ensuring it is systematically considered into strategic and curricular decisions.

Since the previous accreditation, the Lycée has systematically **addressed the recommendations issued**. Measures taken include the optimisation and harmonisation of student questionnaires, the introduction of automated data analysis systems, formalisation of decision-tracking procedures, and strengthening of industry partnerships. Continuous monitoring ensures that feedback is translated into concrete actions, such as the adjustment of course content, the integration of new modules, and preparation for future programme scaling. These steps demonstrate a commitment to continuous improvement and accountability.

The panel commends the program's strong culture of continuous improvement, notably its effective use of student and employer feedback to adapt courses, select external speakers, and refine projects. The emphasis on practical projects, the development of soft skills, and a very motivated, competent teaching staff constitute key strengths of the programme. At the same time, the panel notes that further structuring of certain processes would help support long-term sustainability and traceability of decisions.

In particular, adopting more systematic approaches to collecting, documenting, and reviewing industry feedback would support the continuity and the potential scalability of the programme. This could include documenting feedback analysis, tracking curricular updates over time, and clarifying the implementation and follow-up of strategic decisions. **The panel also encourages reducing reliance on individual contacts for external engagement, integrating workload considerations into feedback processes, and anticipating potential future programme growth.** Finally, debriefings organised after highly technical sessions delivered by external experts would further strengthen the programme's quality assurance and long-term resilience.

Conclusion

The panel concludes that the BTS Cybersecurity at LGK meets criterion 4. Overall, the Lycée Guillaume Kroll demonstrates a comprehensive and continuously developing quality assurance framework for its BTS programmes. The combination of structured internal evaluation, active stakeholder engagement, and systematic use of feedback ensures that programmes remain relevant, effective, and aligned with both academic standards and labour market needs. Opportunities for further enhancement relate mainly to strengthening the structuring of certain processes in order to support long-term continuity, while preserving the flexibility and responsiveness that characterise current practices.

4 Judgement

Following the comprehensive investigation into the quality of the BTS Cybersecurity, the panel concludes that the programme meets all four assessment areas. Consequently, the panel recommends a re-accreditation.

The panel recognises the sustained commitment of the programme staff in developing and refining the curriculum in response to feedback from students, employers, and previous evaluations. These efforts—including the thoughtful adaptation of courses, well-chosen external interventions, and engaging practical projects—demonstrate a strong culture of continuous improvement and high educational standards. The programme is closely aligned with professional needs, and the systematic use of student questionnaires, employer input, and informal feedback reflects a proactive and responsive approach. The panel particularly commends collaborative spirit of the staff, their active engagement in quality assurance, and their ability to create a motivating and supportive learning environment. At the same time, the panel encourages further structuring of certain decision-making and documentation processes in order to consolidate these excellent practices for the future.

Overall, the panel finds that the quality of the programme has been demonstrated in a verifiable manner for the four assessment areas: 1 'Aims and objectives of the study programme', 2 'Admission, evaluation and certification', 3 'Implementation of the programme' and 4 'Quality assurance measures. In light of its overall positive assessment, the panel invites the programme to consider the following **recommendations** for further development:

- Assessment area 1: **Introduce post-session debriefings for highly technical external expert interventions** to maximize pedagogical impact.
- Assessment area 1: **Enhance guidance on progression to Bachelor programmes by providing** more accessible information and structured support to help students navigate these pathways.
- Assessment area 2: **Further strengthen the visibility and promotion of the BTS** to attract a wider and more diverse pool of prospective candidates and to enhance awareness of the programme.
- Assessment area 3: **Strengthen team resilience** by reducing dependency on key individuals through improved internal knowledge sharing, documentation of practices, and mentoring within the teaching team.
- Assessment area 4: **Adopt more systematic approaches to analysing and documenting student and employer feedback**, ensuring that curricular updates and strategic decisions are clearly recorded and followed up.

In conclusion, the panel recommends the re-accreditation of the BTS Cybersecurity programme.

Assessment area		Judgement
1	Aims and objectives of the study programme	MET

2	Admission, evaluation, certification	MET
3	Implementation of the programme	MET
4	Quality assurance measures	MET
	Overall judgement	**Re-accreditation advice**

5 Annexes

5.1 Annex 1 – Composition of the panel

- Mr Nicolas Navet (chair), Professor in the Department of Computer Science (University of Luxembourg);
- Mr Yoann Klein, Senior Cyber Security Advisor, Huawei;
- Ms Ann Das, Lecturer IT-Organisation & Project Management, AI Business Architect, Hogeschool PXL;
- Mr Koen De Bruyne, Bachelor's student in Cybersecurity at Howest University of Applied Sciences.

The panel was supported by:
- Mr David Corradi, NVAO process coordinator;
- Ms Gwenny Nurtantio, external secretary.

All panel members and the secretary have signed a declaration of independence.

5.2   Annex 2 – Schedule of the site visit

08.15–08.30   Panel arrives at Lycée
08.30–08.45   Closed panel meeting
08.45–09.35   Dialogue with management/coordination of the Lycée and the programme
09.35-09.55   Closed panel meeting
09.55–10.55   Dialogue with teaching staff / support staff
10.55–11.15   Closed panel meeting / break
11.15–11.45   Tour of the facilities
11.45–12.00   Closed panel meeting
12.00–13.00   Light lunch / closed panel meeting
13.00–14.00   Dialogue with employers and alumni
14.00–14.20   Closed panel meeting / break
14.20–15.20   Meeting with students
15.20–15.30   Closed panel meeting / break
15.30–16.00   Backup time: meeting with programme management
16.00–17.00   Closed panel meeting
17.00–17.30   Mutual dialogue programme management & panel regarding the findings
                    of the day

5.3 Annex 3 – Documents reviewed

- Accreditation file
- Annexes to the request for accreditation
    a) Rapport d'évaluation 2021
    b) Fiches de cours
    c) Internship Final Grading
    d) Vadémécum

5.4   Annex 4 – Abbreviations used

CYB	Cybersecurity
BTS	Brevet de Technicien Supérieur
ECTS	European Credits Transfer System
EQF	European Qualifications Framework (EQF)
LGK	Lycée Guillaume Kroll
VAE	Validation des Acquis de l'Expérience

Colophon

Lycée Guillaume Kroll
BTS Cybersecurity - (LU01A-25)
Programme Assessment

Final report submitted to the Ministry of Research and Higher Education on 28 January 2026