Annex No. 3

NATIONAL CENTER FOR EDUCATIONAL QUALITY ENHANCEMENT

Accreditation Expert Group Final Report on Higher Education Programme

Joint English-language Cybersecurity Master's Programme

British University and Georgian Technical University

Evaluation Date(s): 18-19 February 2026

Report Submission Date 08 April 2026

Tbilisi

Information about a Higher Education Institution [1]

Name of Institution Indicating its Organizational Legal Form	LLC British University LEPL Georgian Technical University
Identification Code of Institution	405365698 211349192
Type of the Institution	Universities

Expert Panel Members

Chair (Name, Surname, HEI/Organisation, Country)	Seifedine Kadry, LAU Lebanon and Noroff Norway
Member (Name, Surname, HEI/Organisation, Country)	Magda Tsintsadze, LEPL Ivane Javakhishvili Tbilisi State University, Georgia
Member (Name, Surname, HEI/Organisation, Country)	Lia Kurtanidze, Georgian National University, LTD, Georgia
Member (Name, Surname, HEI/Organisation, Country)	Tamta Tskhovrebadze, International Black Sea University LLC, Georgia
Member (Name, Surname, HEI/Organisation, Country)	Tamar Tkhelidze, East European University, LTD, Georgia

[1] In the case of joint education programme: Please indicate the HEIs that carry out the programme. The indication of an identification code and type of institution is not obligatory if a HEI is recognised in accordance with the legislation of a foreign country.

I. Information on the education programme

Name of Higher Education Programme (in Georgian)	კიბერუსაფრთხოება
Name of Higher Education Programme (in English)	Cybersecurity
Level of Higher Education/programme	7
Qualification to be Awarded[2]	Master of Cybersecurity
Name and Code of the Detailed Field	0613 Software and Applications Development and Analysis
Indication of the right to provide the teaching of subject/subjects/group of subjects of the relevant cycle of the general education[3]	
Language of Instruction	English
Number of ECTS credits	120
Programme Status (Accredited/ Non-accredited/ Conditionally accredited/ Newly proposed/International accreditation) Indicating Relevant Decision (number, date)	New
Additional requirements for the programme admission (in the case of an art-creative and/or sports educational programme, passing a creative tour/internal competition, or in the case of another programme, specific requirements for admission to the programme/implementation of the programme)	
The quota for MD students requested by the HEI (In the case of Medical Doctor one-cycle educational programme)	

[2] In case of implementing a joint higher education programme with a higher education institution recognized in accordance with the legislation of a foreign country, if the title of the qualification to be awarded differs, it shall be indicated separately for each institution.

[3] In case of Integrated Bachelor's-Master's Teacher Training Educational Programme and Teacher Training Educational Programme

II. Accreditation Report Executive Summary

- **General Information on Education Programme**

The joint Master's programme in Cybersecurity is a newly established programme developed through a partnership between the British University and the Technical University of Georgia, representing the next stage of their successful academic collaboration. The programme aligns with the missions of both institutions by preparing graduates to act effectively, ethically, and flexibly in an increasingly digital and globally connected environment. The programme spans two academic years and totals 120 ECTS credits. It includes 100 ECTS credits of compulsory cybersecurity courses, 20 ECTS credits of elective courses, and 30 ECTS credits dedicated to the master's thesis. The curriculum is designed in response to local and international labor market demands, ensuring that graduates acquire the knowledge and competencies needed to compete globally. The relevance of the programme is supported by market research, which highlights the growing demand for cybersecurity professionals. Rapid digital transformation, the expansion of artificial intelligence, cloud computing, and the protection of critical infrastructures have made cybersecurity a central component of national security, economic stability, business competitiveness, and public trust. As cyber threats and data breaches increase, the need for highly skilled cybersecurity specialists continues to grow. The programme is delivered in English and follows modern educational standards and international best practices. Its development considered sectoral cybersecurity education guidelines issued by EQE, as well as international accreditation standards such as ABET and ACM. Additionally, the curriculum was informed by a comparative analysis of cybersecurity master's programmes offered by leading universities worldwide, ensuring alignment with global academic and professional standards.

- **Overview of the Accreditation Site Visit**

The evaluation of the program was carried out on February 18 and 19, 2026, by the expert panel approved by the order of the NCEQE. The format of the evaluation was physical, with Georgian experts and representatives of the institution attending interviews on-site, as well as the chair of the panel from abroad. Accreditation experts held a preliminary meeting online on February 12, where they shared their preliminary findings based on the review of the program, self-evaluation report, and relevant annexes and planned the details of the evaluation. The expert panel had the chance to meet all internal and external stakeholders of the program and observe material-technical resources. Namely, the expert panel held interviews with the two universities and their faculty administrations, the self-evaluation team, representatives of the quality assurance office, heads of the program, academic and invited staff of the program, students and alumni from another program, and employers. The

Accreditation visit was well organized, and the working environment was collaborative and welcoming.

- **Brief Overview of Education Programme Compliance with the Standards**

Standard 1: Substantially Complies with Requirements

- Substandard 1.1, 1.5 Complies with Requirements
- Substandard 1.2, 1.3, 1.4 Substantially Complies with Requirements

Standard 2: Substantially Complies with Requirements

- Substandard 2.1, 2.2 Substantially Complies with Requirements
- Substandard 2.3, 2.4 Complies with Requirements

Standard 3: Complies with Requirements

- Substandard 3.1 Complies with Requirements
- Substandard 3.2 Substantially Complies with Requirements

Standard 4: Complies with Requirements

- Substandard 4.1-4.5 Complies with Requirements

Standard 5: Complies with Requirements

- Substandard 5.1-5.3 Complies with Requirements

Recommendations

1.2 Programme Learning Outcomes

- It is recommended that outcomes 2 and 4 be adjusted to align with the qualification level and be formulated in a measurable way.
- It is recommended that a consistent document be adapted for the outcomes wording.
- -It is recommended to explicitly include elements related to continuous professional development and contributions to advancing cybersecurity knowledge and practice, which are important aspects of modern cybersecurity education frameworks.

1.3 Evaluation Mechanism of the Programme Learning Outcomes

- It is recommended that a rubric be developed, when needed, for each performance indicator. The rubric's language must align with the performance indicator. Clearly

select the courses to be used for assessment of the performance indicators. Fixing the matrix in the file Cyb Map Eng (Appendix 1).
- Unify the assessment mechanism between the two universities.

1.4 Structure and Content of Educational Programme

- It is recommended that the following topics be added as required: Cybercrime, cyber policy, and Global cybersecurity governance.

2.1 Programme Admission Preconditions

- The programme should clearly define and formally document minimum prerequisite competencies required for admission, particularly in core computing areas such as programming, operating systems, computer networks, discrete mathematics, and cybersecurity fundamentals.
- The institution should establish and formalize a bridging or preparatory mechanism for applicants from non-computer science backgrounds to ensure equitable achievement of programme learning outcomes

2.2. The Development of practical, scientific/research/creative/performing and transferable skills

- Formally approve and publish the Master's Thesis syllabus and supervision guidelines
- Develop joint research supervision mechanisms between partner institutions.

3.2. Master's Students Supervision

- It is recommended to develop a specific regulation for the joint Master's Program that comprehensively defines the procedures for the selection, appointment, and replacement of supervisors/co-supervisors, clarifies their rights and responsibilities, establishes a transparent methodology for determining the supervisor-to-student ratio, and regulates all other relevant aspects necessary for the effective implementation of the program.
- Define supervisor workload limits and supervisor-to-student ratio

Suggestions

1.5. Academic Course/Subject

Some course titles are inconsistent across the documents, possibly due to typos.

2.1 Programme Admission Preconditions

- A structured diagnostic assessment mechanism is suggested to be introduced at the admission stage to verify applicants' preparedness for Level 7 study requirements
- The program may consider restricting eligibility primarily to applicants with computing-related Bachelor's degrees or clearly equivalent academic preparation.
- Periodic review of admission examination content based on student performance data may further strengthen alignment between entry competencies and program demands
- Introducing a formal academic advising session for newly admitted students to assess individual preparedness could support smoother academic integration
- The professional admission examination may be explicitly aligned with these prerequisite competencies and structured to assess technical readiness for advanced cybersecurity coursework
- Admission criteria and competency expectations maybe publicly accessible and clearly communicated to prospective applicants

2.2. The Development of practical, scientific/research/creative/performing and transferable skills

- Introduce research-based mini-projects within technical courses.
- Encourage integration of students into ongoing faculty research projects.

2.3. Teaching and learning methods

- Strengthen integration of research-based and analytical tasks within technical courses to better reflect Master-level expectations.
- Introduce advanced integrative projects requiring synthesis of multiple cybersecurity domains.
- Encourage greater incorporation of comparative analysis of tools, frameworks, and methodologies within technical coursework

4.1 Human Resources

- The universities may improve the qualifications of academic staff in cybersecurity by involving and developing specialists who have both strong theoretical knowledge and practical experience in this field.

4.2 Qualification of Supervisors of Master's Students

- The universities may increase the number of qualified academic staff eligible to supervise master's theses, particularly in cybersecurity, and strengthen the involvement of personnel holding doctoral degrees to ensure adequate supervision capacity for the planned student enrollment.

4.3 Professional development of academic, scientific and invited staff

- It is suggested to strengthen academic and research activities in the field of cybersecurity within the program, including increasing the number of publications in international peer-reviewed journals, enhancing participation in specialized conferences, expanding academic mobility, and organizing targeted workshops and training sessions.
- It is suggested to increase field-specific activities at the British university.

Brief Overview of the Best Practices (if applicable)[4]

- **Information on Sharing or Not Sharing the Argumentative Position of the HEI**

The expert team partially agrees with the university's argumentative position. Specifically, the following recommendations are moved to suggestions with updated wording:

- The professional admission examination may be explicitly aligned with these prerequisite competencies and structured to assess technical readiness for advanced cybersecurity coursework

- Admission criteria and competency expectations may be publicly accessible and clearly communicated to prospective applicants

-The universities may improve the qualifications of academic staff in cybersecurity by involving and developing specialists who have both strong theoretical knowledge and practical experience in this field.

-The universities may increase the number of qualified academic staff eligible to supervise master's theses, particularly in cybersecurity, and strengthen the involvement of personnel holding doctoral degrees to ensure adequate supervision capacity for the planned student enrollment.

Other recommendations remained unchanged because they are not in compliance with their sub-standards.

[4] A practice that is exceptionally effective and that can serve as a benchmark or example for other educational programme/programmes.

- **Quantitative Data Analysis of the educational programme in accordance with the requirements of the accreditation standards, for** example:

  - **Staff and Supervisors** - Number of the staff involved in the programme (including academic, scientific, international and invited staff), including the staff holding PhD degree in the sectoral direction; ratio of the academic/scientific staff and invited staff; ratio of the affiliated and academic staff; ratio of Master's students to supervisors; supervisors' workload scheme;

    The Master's programme is implemented by a qualified academic and scientific staff with relevant expertise in the sectoral field. In total, 14 academic staff members are involved in the delivery of the programme. All of them possess sectoral expertise relevant to the programme, and 8 members hold a PhD degree in the sectoral direction. Importantly, all 14 academic staff members are affiliated with the university, ensuring institutional stability and continuity in programme implementation.
    The academic staff structure includes 8 Professors, 2 Associate Professors, and 4 Assistant Professors. Among the Professors, all eight possess doctoral degrees in the relevant field. Within the Associate Professor category, one staff member holds a PhD degree in the sectoral direction, while among the Assistant Professors all four possess doctoral qualifications relevant to the field. No assistant-level academic staff are involved in the programme.
    In addition to the academic staff, the programme benefits from the contribution of 8 scientific staff members, who support research-related activities and contribute to strengthening the research environment of the programme. The programme also includes one international staff member, who contributes to the internationalization of teaching and research activities.
    There is no visiting academic staff currently involved in the programme. Therefore, the programme is primarily delivered by affiliated academic staff, ensuring consistency in teaching, supervision, and academic development.

  - **Scientific/Research Indicators** - Scientific/research index of the individuals, involved in the programme (for the last 5 years): quantitative data papers published in peer-reviewed journals with an international index; Staff participation rates in local and international conferences; other scientific/research indicators;
    The academic staff involved in the programme demonstrate ongoing engagement in scientific and research activities, particularly through participation in international conferences, scientific-practical forums, and publication of research results in peer-reviewed journals and conference proceedings. The available evidence indicates that the programme staff maintains **active but moderate research activity**. The strongest elements of the research profile include:
    regular participation in international scientific conferences, involvement in interdisciplinary research topics related to artificial intelligence and digital technologies, international academic mobility, and collaboration within European programmes.

However, the research output is **primarily concentrated in conference presentations and a limited number of journal publications**, suggesting that further development of high-impact journal publications and externally funded research projects would strengthen the programme's scientific profile. The CVs provided by the program didn't clearly mention the publication types, if any, and the committee wasn't able to provide a quantitative analysis for this section.

- **Academic Staff Turnover Rate** (for the last 5 years) (e.g. the number of retired staff, the number of staff who left the institution and the number of new staff, etc.);
  N/A
- **Data on the Individuals Enrolled** (for the last 5 years; in case of active programmes); number of student places announced for the programme; student progression by academic years;
  N/A
- **Analysis of other quantitative data** provided in the self-assessment and annexes.

▪ **In case of re-accreditation, a brief overview of significant achievements and/or progress (if applicable) during the accreditation period, as well as a review of the fulfillment of the recommendations received during the previous evaluation process.**

III. Summary Table of Compliance of the programmes with the standards

	Standard	Evaluation
1.	**1.1. Educational Programme Objectives, Learning Outcomes and their Compliance with the Programme**	**Substantially**
1.1	Programme Objectives	**Complies**
1.2	Programme Learning Outcomes	**Substantially**
1.3	Evaluation Mechanism of the Programme Learning Outcomes	**Substantially**
1.4	Structure and Content of Educational Programme	**Substantially**
1.5	Academic Course/Subject	**Complies**
2.	**Methodology and Organization of Teaching, Adequacy of Evaluation of Programme Mastering**	**Substantially**
2.1	Programme Admission Preconditions	**Substantially**
2.2	The Development of Practical, Scientific/Research/ Creative/ Performance and Transferable Skills	**Substantially**
2.3	Teaching and Learning Methods	**Complies**
2.4	Student Evaluation	**Complies**
3.	**Student Achievements and Individual Work with Them**	**Complies**
3.1	Student Consulting and Support Services	**Complies**
3.2	Master's Student Supervision	**Substantially**
4	**Providing Teaching Resources**	**Complies**
4.1	Human Resources	**Complies**
4.2	Qualification of Supervisors of Master's Student	**Complies**
4.3	Professional Development of Academic, Scientific and Invited Staff	**Complies**
4.4	Material Resources	**Complies**
4.5	Programme/Faculty/School Budget and Programme Financial Sustainability	**Complies**
5	**5. Teaching Quality Enhancement Opportunities**	**Select Appropriate**
5.1	Internal Quality Evaluation	**Complies**
5.2	External Quality Evaluation	**Complies**
5.3	Programme Monitoring and Periodic Review	**Complies**

Guidelines and Standards (See link)

Accreditation Standards for Higher Education Programmes

Guideline for Assessment of Accreditation Standards of Higher Education Programmes

Suggestions on the evaluation of the methodology for determining the threshold number of student quotas on a higher education institution educational programme of a certified medical doctor

Assessment criteria

Definitions:
Recommendations - should be considered by the HEI in order to comply the programme with the requirements of the standard
Suggestions - non-binding suggestions for the programme development

IV. Compliance of the Programme with Accreditation Standards

1. Educational Programme Objectives, Learning Outcomes and their Compliance with the Programme

A programme has clearly established objectives and learning outcomes, which are logically connected to each other. Programme objectives are consistent with the mission, objectives and strategic plan of the HEI. Programme learning outcomes are assessed on a regular basis to improve the programme. The content and consistent structure of the programme ensure the achievement of the set goals and expected learning outcomes.

1.1 Programme Objectives

Programme objectives consider the specificity of the field of study, level and educational programme, and define the set of knowledge, skills and competences a programme aims to develop in graduate students. They also illustrate the contribution of the programme to the development of the field and society.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The programme objectives are generally clearly formulated and achievable. The programme states that its purpose is to train cybersecurity specialists with both theoretical and practical competencies relevant to international market requirements.

Furthermore, the documentation and interviews indicates that a mapping between programme goals and learning outcomes has been developed, demonstrating that the intended outcomes are aligned with the programme objectives. This alignment suggests that the objectives are operationalized through measurable learning outcomes, which is consistent with EQE expectations.

The objectives clearly reflect the specific characteristics of the cybersecurity field. They emphasize: analysis of vulnerabilities and cyber threats, development of secure cyber infrastructures, implementation of organizational cybersecurity systems, research in cybersecurity using modern methodologies.
These elements correspond well to the advanced knowledge and analytical competencies expect+ed at the Master's level, particularly the inclusion of independent research and application of advanced methods.

The objectives explicitly indicate that graduates will develop:

- advanced theoretical knowledge in cybersecurity,
- practical skills in threat analysis and infrastructure protection,
- research competencies, and
- ethical awareness and academic integrity.

These elements correspond to the knowledge–skills–competence framework required by the Georgian National Qualifications Framework for Master's programmes.

The programme objectives reference the preparation of specialists who will contribute to: organizational cybersecurity protection, and the development of the cybersecurity field and society. This aligns with the missions of the participating universities and with the societal importance of cybersecurity.

The programme objectives are explicitly linked to the missions of both partner institutions:

- British University: preparing graduates for successful action in a globally connected world.

- Georgian Technical University: promoting intellectual, cultural, and socio-economic development and preparing competitive specialists.

The programme's emphasis on innovation, international competitiveness, and lifelong learning aligns well with these institutional missions.

The programme states that: cybersecurity professionals are in high demand globally and in Georgia, and labour market analysis and employer consultations were conducted. The involvement of employers and field specialists in workshops during programme development is a positive practice and aligns with EQE expectations regarding stakeholder participation.

The programme addresses internationalization primarily through alignment with international cybersecurity market requirements, and preparation of graduates for the global work environment.

The programme indicates that the objectives will be published through the university website, and other information and communication channels.

The documentation and interviews confirms that the objectives were developed through collaboration involving:

- academic staff,
- administrative staff,
- programme working groups,
- employers and field specialists.

Workshops and consultations were conducted during programme development. This indicates that the objectives are shared among programme stakeholders.

Evidences/Indicators

- Self Study

- Educational programme;
- Mission, objectives and strategy of the HEI, its faculty/school/main educational unit and/or structural unit;
- Analysis of the demands of labour market and employers;
- Website;
- Interview results.

Recommendations:

- Proposal(s), which should be considered by the HEI, the programme to meet the requirements of the standard

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
1.1 Programme Objectives	Complies

1.2 Programme Learning Outcomes

➢The learning outcomes of the programme are logically related to the programme objectives and the specifics of the study field.

➢ Programme learning outcomes describe knowledge, skills, and/or the responsibility and autonomy that students gain upon completion of the programme.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The learning outcomes are logically related to the programme objectives, supported by a programme goals–learning outcomes mapping table. The programme further states that

course-level learning outcomes contribute to programme-level outcomes, which is consistent with EQE expectations for constructive alignment.

The stated learning outcomes reflect several core competencies expected from a cybersecurity graduate, including: analysis of complex cybersecurity problems, development of cybersecurity solutions, professional communication, ethical and legal decision-making, teamwork and leadership, application of cybersecurity principles to ensure operational continuity.

These outcomes broadly correspond to the programme goals of preparing cybersecurity specialists capable of addressing modern security challenges.

The learning outcomes cover several competence dimensions required by the Georgian National Qualifications Framework (NQF) for Master's programmes, including:

Knowledge and analytical competence

- analyzing complex cybersecurity problems;
- applying cybersecurity principles and sectoral standards.

Practical and problem-solving skills

- building and evaluating cybersecurity solutions;
- implementing security measures for operational continuity.

Transferable and professional skills

- communication in professional contexts;
- teamwork and leadership.

Responsibility and ethical awareness

- decision-making based on legal and ethical principles.

The majority of the outcomes are measurable, achievable and realistic, and were developed based on the sectoral characteristics of the field.

The learning outcomes emphasize complex problem solving, design of solutions, ethical decision-making and professional collaboration, which correspond to the expected advanced competencies of a second-cycle qualification.

The programme documentation indicates that the development of the learning outcomes considered the requirements of the labour market and the expectations of relevant stakeholders. In particular, a labour market analysis was conducted, and feedback from employers was taken into account during the design and development of the programme. This process ensured that the programme outcomes reflect the competencies required in professional cybersecurity practice and align with the employment opportunities available to graduates.

The learning outcomes of the programme support graduates' employability by focusing on key professional competencies in the cybersecurity field. These include the ability to analyse cyber threats and vulnerabilities, implement system protection mechanisms, and design and develop cybersecurity solutions that respond to contemporary security challenges faced by organizations.

In addition to preparing graduates for employment in the cybersecurity sector, the programme also provides a foundation for further academic advancement.

The learning outcomes reflect key competencies relevant to cybersecurity practice.

The development of learning outcomes involved: academic staff, students, graduates, employers.
Consultations with these stakeholders occurred during programme development and through programme discussions. This collaborative approach aligns with EQE expectations for participatory programme development. The staff responsible for implementation ensures that the learning outcomes are shared with stakeholders through discussions and programme development processes.

To meet level 7, we recommend to change "2. Builds, develops, and evaluates innovative solutions by meeting the requirements defined in the cybersecurity context;" to "2. Designs,

develops, and evaluates innovative solutions by meeting the requirements defined in the cybersecurity context;". Replace "Understands" in outcome 4 with "Demonstrates" to make it measurable. In addition the outcomes wording is not consistent across the documentations (for example, compare Self Assessment Report and Students Outcomes Assessment Methodology…).

While the proposed programme learning outcomes largely correspond to the sectoral benchmark expectations and cover most of the key areas related to cybersecurity knowledge, practical skills, and professional responsibility, the alignment could be strengthened by explicitly incorporating references to continuous professional development and contribution to the advancement of cybersecurity practice or knowledge. Adding such elements would ensure more complete coverage of the benchmark domains and provide a clearer reflection of the broader competencies expected from graduates in the cybersecurity field.

Evidences/Indicators

- Educational programme
- Map of programme objectives and learning outcomes;
- Analysis of labor market and employer demands;
- Website;
- Interview results.

Recommendations:

- It is recommended that outcomes 2 and 4 be adjusted to align with the qualification level and be formulated in a measurable way
- It is recommended that aconsistent document be adapted for the outcomes wording.
- It is recommended to explicitly include elements related to continuous professional development and contributions to advancing cybersecurity knowledge and practice, which are important aspects of modern cybersecurity education frameworks.

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
1.2 Programme Learning Outcomes	Substantially complies

1.3 Evaluation Mechanism of the Programme Learning Outcomes

- Evaluation mechanisms of the programme learning outcomes are defined; the programme learning outcomes evaluation cycle consists of defining, collecting and analyzing data necessary to measure learning outcomes;
- Programme learning outcomes assessment results are utilized for the improvement of the programme.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

As per the evaluation mechanism provided by GTU, the programme has established a structured methodology for evaluating the achievement of programme learning outcomes. The assessment framework follows a systematic, evidence-based process that integrates direct and indirect evaluation methods. Direct assessment is conducted through the evaluation of student work products such as examinations, laboratory assignments, research projects, and the Master's thesis. Indirect assessment includes feedback from student surveys, alumni surveys, employer feedback, and external evaluations of thesis or capstone projects. This approach is consistent with outcome-based education principles and allows the programme to measure the extent to which students achieve the intended learning outcomes. Such mechanisms align with the expectations of EQE accreditation standards, which require institutions to define, collect, and analyse relevant data to measure programme learning outcomes in a consistent and transparent manner. As this is a joint program, it is recommended that both universities develop or agree on a unified assessment mechanism.

The programme has defined Student Outcomes (SOs) and associated Performance Indicators (PIs) that operationalize the learning outcomes and make them measurable. Each learning outcome is supported by multiple performance indicators that describe the specific competencies students must demonstrate. The programme also employs standardized rubrics using a five-level attainment scale, which helps ensure consistency and transparency in the evaluation process across courses and cohorts. Furthermore, the development of a course–outcome–performance indicator matrix demonstrates systematic alignment between programme learning outcomes and the curriculum components that support their achievement. This mapping approach corresponds to good practices recommended in accreditation processes, where learning outcomes are assessed through the programme components responsible for developing them.

Despite the program developing performance indicators for each outcome to make it measurable, the rubric provided is for the outcome rather than the performance indicator. We recommend developing a rubric, when needed, for each performance indicator. The rubric's language must align with the performance indicator. For example, for the PI: Identifies key elements and constraints of a complex cybersecurity problem, we recommend this rubric:

Level	Descriptor	Performance Description
4 – Exemplary	Comprehensive identification	Correctly identifies all major elements of the cybersecurity problem, including system components, threat actors, vulnerabilities, attack vectors, environmental conditions, and operational constraints (technical, legal, organizational). Demonstrates deep understanding of the problem context and relationships among elements.
3 – Proficient	Adequate identification	Identifies most key elements and major constraints of the cybersecurity problem. Demonstrates good understanding of the system context but may omit some secondary elements or constraints.

2 – Developing	Partial identification	Identifies some relevant elements of the cybersecurity problem but misses several important components or constraints. Understanding of the problem context is incomplete or superficial.
1 – Beginning	Limited identification	Identifies few or incorrect elements of the cybersecurity problem. Shows minimal understanding of relevant constraints or the overall problem context.

Additionally, the program must clearly select the course(s) where each PI will be assessed. Also, the mapping coverage matrix in Appendix 1 appears to be inaccurate, for example outcome 6, covered immediately with Strength (3) where the introduction (1) is missing. Other outcomes start by deepening (2) then later in the curriculum was introduced. Such inaccuracies will make the assessment wrong or misleading. If the assessment mechanism follows GTU, the BU staff needs to be trained accordingly and vice versa.

The programme has also established benchmarks for outcome attainment. According to the methodology, a learning outcome is considered achieved when at least 70% of students reach a satisfactory level (level 3 or higher) for each performance indicator, and at least 25% of students achieve a higher level of performance (level 4 or above). The existence of such quantitative benchmarks demonstrates that the programme has defined measurable standards for evaluating student achievement and enables the monitoring of learning outcomes over time.

The evaluation process is coordinated by the Self-Assessment Team (SAT) and a Quality Assurance Specialist, who oversee the implementation of the assessment plan, collect and analyse data, and prepare summary reports on outcome attainment. The programme follows an annual assessment cycle that includes planning, data collection during the semester, analysis of results at the end of the semester, and the preparation of assessment reports. The results are reviewed by the programme's self-assessment team, and identified weaknesses

trigger corrective actions such as curriculum revisions, improvements in laboratory work, updates to assessment rubrics, or other modifications to programme components. This process reflects the principle of continuous quality improvement, which is a key requirement of the accreditation framework.

The programme also demonstrates the engagement of external stakeholders in the evaluation of learning outcomes. Employer feedback, alumni surveys, internship evaluations, and external reviewers of the Master's thesis are used as indirect assessment mechanisms. These mechanisms contribute to verifying whether the competencies acquired by students correspond to the expectations of the labour market and professional community.

Additionally, the programme ensures that academic and visiting staff involved in teaching are informed about the assessment methodology. Instructors are notified at the beginning of each semester regarding the courses selected for assessment and the learning outcomes to be evaluated. They are provided with assessment templates, rubrics, and guidelines prepared by the quality assurance unit, which supports the consistent implementation of evaluation procedures.

The programme also maintains a structured documentation and reporting system. Assessment data, rubrics, course evidence, and improvement actions are stored in an assessment repository, and annual assessment reports summarize the attainment of programme outcomes and identify trends over time. These reports serve as the basis for programme improvement and strategic decision-making.

Evidences/Indicators

- Programme learning outcomes assessment mechanism
- Plan of evaluation for learning outcomes of educational programme
- Curriculum map;
- Benchmarks;
- Interview results.

Recommendations:

- - It is recommended that a rubric be developed , when needed, for each performance indicator. The rubric's language must align with the performance indicator.
- It is recommended to clearly select the courses to be used for assessment of the performance indicators. Fixing the matrix in the file Cyb Map Eng (Appendix 1).
- It is recommended to unify the assessment mechanism between the two universities.

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
1.3 Evaluation Mechanism of the Programme Learning Outcomes	Substantially complies

1.4. Structure and Content of Education Programme

- The Programme is designed according to HEI's methodology for planning, designing and developing of education programmes.
- The Programme structure is consistent and logical. The content and structure of the programme ensure the achievement of programme learning outcomes. The qualification to be granted is consistent with the content and learning outcomes of the programme.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The programme was developed in accordance with the institutional regulations of the university, specifically the Rules and Procedures for the Development, Approval, Modification and Cancellation of Educational Programmes. The documentation indicates that the programme design followed the established institutional methodology and that its development was coordinated jointly by the partner institutions.

According to EQE standards, higher education institutions must have a defined methodology that determines the procedures, responsibilities, and stages involved in programme development and ensures the involvement of relevant stakeholders.

Based on the provided information, the programme development process appears to be consistent with these requirements, as academic and administrative staff from the participating universities collaborated in designing the programme structure, concept, and partnership agreement.

The programme is designed as a Master's degree programme with a total volume of 120 ECTS credits delivered over two academic years. This structure corresponds to the standard second-cycle higher education model within the European Higher Education Area, where one academic year typically represents approximately 60 ECTS credits.

The programme includes:

- 100 ECTS credits of compulsory courses in the major field of study,
- 30 ECTS credits allocated to the Master's thesis, and
- 20 ECTS credits of elective courses.

The inclusion of a substantial research component (Master's thesis) is consistent with expectations for Master's level programmes, where students are expected to develop analytical and research competencies. The overall volume, complexity and research components of the programme therefore correspond to the second cycle of higher education and the relevant qualification level.

The programme structure is designed using the European Credit Transfer and Accumulation System (ECTS) and complies with the relevant legislative requirements governing higher education programmes in Georgia. The programme documentation confirms that the curriculum and programme implementation follow both national regulations and the internal quality assurance procedures of the partner institutions.

The use of ECTS ensures transparency in student workload, supports student mobility, and aligns the programme with the European Higher Education Area framework.

The content and structure ensure the individuality of the programme, particularly through its joint implementation by two higher education institutions and the integration of expertise from both partners. The joint delivery model, which allows courses to be taught on the campuses of both institutions by their respective academic staff, contributes to the distinctiveness of the programme.
the programme structure and content are logically organized and aligned with the programme learning outcomes. The courses included in the curriculum are designed to contribute to the development of the competencies required for cybersecurity professionals, and the programme integrates both theoretical knowledge and practical skills. The programme structure appears to be logically organized, with courses arranged in a sequence that supports the gradual development of knowledge and skills. The programme components are interconnected and that their content develops progressively throughout the programme.

Furthermore, course prerequisites are described in a logical manner, ensuring that students possess the necessary foundational knowledge before progressing to more advanced components. This sequential structure is consistent with EQE expectations that programme components be logically organized and coherently structured.

The curriculum is based on sectoral benchmarks, recent research findings, and modern achievements in cybersecurity. This is particularly important for a Master's programme, where teaching should reflect current developments in the discipline and support research-based learning. The programme includes elements that support internationalization. The programme's development involved collaboration between academic staff and administrative units at the participating universities. The programme was developed through a collaborative process involving relevant stakeholders. The information about the programme is made publicly available through institutional communication channels.
A couple of topics are missing across the curriculum, therefore to be fully aligned with the sectoral benchmark, the panel recommends adding the following topics as required: Cybercrime, Cyber policy, and Global cybersecurity governance.

Evidences/Indicators

- Methodology and/or rule for planning, designing and developing educational programmes;
- Educational programme with the enclosed syllabi;
- Curriculum map;
- Website;
- Interview results.

Recommendations:

- It is recommended that the following topics be added as required: Cybercrime, cyber policy, and Global cybersecurity governance.

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
1.4 Structure and Content of Educational Programme	Substantially complies

1.5. Academic Course/Subject

➢ The content of the academic course / subject and the number of credits ensure the achievement of the learning outcomes defined by this course / subject.
➢ The content and the learning outcomes of the academic course/subject of the main field of study ensure the achievement of the learning outcomes of the programme.
➢ The study materials indicated in the syllabus ensure the achievement of the learning outcomes of the programme.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The learning outcomes of each academic course are aligned with the learning outcomes of the programme. This alignment is reflected in the programme competency map, which shows how individual courses contribute to the achievement of programme-level learning outcomes. According to EQE accreditation guidelines, each course should explicitly demonstrate its contribution to one or more programme learning outcomes through a curriculum mapping mechanism that ensures the coherence of the programme structure.
Based on the information provided, each course contributes to at least one programme learning outcome, and course learning outcomes are formulated considering the thematic content of the course.

The content of each course is designed according to the learning outcomes defined for that course. The syllabi of the courses include clearly defined topics, learning outcomes, and assessment mechanisms that correspond to the intended competencies developed within the course. EQE guidelines emphasize that course content must directly support the achievement of course learning outcomes and, consequently, contribute to programme learning outcomes, the documentation, the courses appear to follow this principle.

The number of ECTS credits assigned to each course is determined by considering the course content, expected learning outcomes, and student workload. The programme documentation indicates that both **contact hours and independent study hours** are taken into account when determining the credit allocation for each course. The programme also reports that the ratio between contact hours and independent learning hours reflects the specific characteristics of each course and supports the achievement of course learning outcomes.

The learning outcomes defined within each course are evaluated using the assessment components described in the course syllabi. These components include examinations, assignments, and other evaluation mechanisms defined in the course assessment system. Based on the description provided, the programme has established a structured evaluation system within the syllabi. the syllabi include modern and up-to-date literature that corresponds to the content of each course and reflects developments in the field of cybersecurity. The listed literature and learning resources are described as relevant to the course content and aligned

with the intended learning outcomes. The laboratories meet the requirements to achieve the program learning outcomes.

Evidences/Indicators

- Educational programme with enclosed syllabi;
- Curriculum map;
- Course learning outcomes assessment results;
- Results of the interview.
- Educational programme, teaching materials/resources, databases of international electronic library indicated in the attached syllabi;

Recommendations:

- Proposal (s), which should be considered by the HEI, the programme to meet the requirements of the standard

Suggestions for the Programme Development

- Some course titles are not consistent among the documents, maybe due to typos.

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
1.5. Academic Course/Subject	Complies

2. Methodology and Organisation of Teaching, Adecuacy of Evaluation of Programme Mastering

Prerequisites for admission to the programme, teaching-learning methods and student assessment consider the specificity of the study field, level requirements, student needs, and ensure the achievement of the objectives and expected learning outcomes of the programme.

2.1 Programme Admission Preconditions

The HEI has relevant, transparent, fair, public and accessible programme admission preconditions and procedures that ensure the engagement of individuals with relevant knowledge and skills in the programme to achieve learning outcomes.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

Admission to the Master's Programme in Cybersecurity is conducted in accordance with national legislation and institutional regulations . Applicants are required to hold a Bachelor's degree in a STEM field and successfully pass the Unified Master's Examination, as well as English language and professional assessments determined by the institution.

Admission procedures are publicly described and formally regulated. The programme language is English, and language competence requirements are specified.

However, during the review of the documentation and interviews, the expert panel identified a structural concern regarding academic preparedness of admitted students.

The admission criteria allow applicants with a general STEM background. While this is formally acceptable, the programme documentation does not clearly define:

Minimum required prior knowledge in:

- Programming
- Operating Systems
- Computer Networks
- Discrete Mathematics
- Cybersecurity fundamentals

Furthermore, the programme does not demonstrate the existence of bridging or leveling mechanisms for candidates from non-computer science backgrounds. In the absence of clearly defined academic prerequisites or compensatory preparatory modules, there is a structural risk that admitted students may not possess the necessary technical foundation to successfully engage with advanced cybersecurity coursework.

Given that the curriculum includes technically demanding subjects such as Penetration Testing, Malware Analysis, and Intrusion Detection and Auditing, admission of students without a solid computing background may compromise the effective achievement of programme learning outcomes. This may also affect the programme's ability to consistently deliver Level 7 academic depth, particularly in courses requiring advanced analytical reasoning and system-level understanding.

Additionally, lack of a structured diagnostic assessment of technical competency may result in heterogeneous student preparedness levels within the cohort. This may impact instructional efficiency, necessitate unplanned remediation, and potentially dilute the academic rigor expected at Master's level.

For a specialized Master's programme in Cybersecurity, it is essential to clearly define and publicly communicate minimum technical competency requirements and, where necessary, provide structured preparatory pathways to ensure that all admitted students are capable of achieving the intended learning outcomes.

Evidences/Indicators

- Component evidences/indicators, including the relevant documents and interview results

Recommendations:

- The programme should clearly define and formally document minimum prerequisite competencies required for admission, particularly in core computing areas such as programming, operating systems, computer networks, discrete mathematics, and cybersecurity fundamentals
- The institution should establish and formalize a bridging or preparatory mechanism for applicants from non-computer science backgrounds to ensure equitable achievement of programme learning outcomes

Suggestions for the Programme Development

- A structured diagnostic assessment mechanism is suggested to be introduced at the admission stage to verify applicants' preparedness for Level 7 study requirements
- The program may consider restricting eligibility primarily to applicants with computing-related Bachelor's degrees or clearly equivalent academic preparation.
- Periodic review of admission examination content based on student performance data may further strengthen alignment between entry competencies and program demands
- Introducing a formal academic advising session for newly admitted students to assess individual preparedness could support smoother academic integration
- The professional admission examination should be explicitly aligned with these prerequisite competencies and structured to assess technical readiness for advanced cybersecurity coursework
- Admission criteria and competency expectations should be publicly accessible and clearly communicated to prospective applicants

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
2.1 Programme Admission Preconditions	Substantially complies

2.2. The Development of Practical, Scientific/Research/Creative/Performing and Transferable Skills

Programme ensures the development of students' practical, scientific/research/creative/performing and transferable skills and/or their involvement in research projects, in accordance with the programme learning outcomes.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The Master's Programme in Cybersecurity demonstrates a strong practical orientation consistent with the specificity of the study field. The curriculum includes laboratory-intensive technical courses such as Penetration Testing, Malware Analysis, Intrusion Detection and Auditing, and Cloud Security. These courses integrate applied exercises, simulated attack scenarios, and controlled system analysis tasks designed to develop practical competencies aligned with the programme learning outcomes.

During the site visit, the Panel was provided with a demonstration of the cybersecurity laboratory environment, that is operational and appropriate for delivering the practical components of the programme.
In addition to practical skills, the programme incorporates research-oriented components through a dedicated Research Methods and Academic Writing course and 30 ECTS Master's thesis requirements. These elements provide a framework for the development of scientific and transferable skills, including critical thinking, professional communication, and ethical reasoning.
While the thesis component exists and supervision procedures were described during the visit, the experts did not receive a formally approved thesis syllabus and detailed supervision guidelines as part of the documentation package and the clear written regulations defining research expectations, criteria for originality and innovation also the Supervisor-to-student ratio limits.
The programme involves multiple academic staff members, however, clear documentation linking faculty research specialization to defined thesis areas was not formally presented.
Given that only a limited number of faculty demonstrate strong cybersecurity-specific research profiles, structured supervision allocation and workload regulation are essential.

Evidences/Indicators

- Component evidences/indicators, including the relevant documents and interview results

Recommendations:

- Develop joint research supervision mechanisms between partner institutions
- Formally approve and publish the Master's Thesis syllabus and supervision guidelines

Suggestions for the Programme Development

- Introduce research-based mini-projects within technical courses.
- Encourage integration of students into ongoing faculty research projects.
-

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
2.2. The Development of practical, scientific/research/creative/performing and transferable skills	Substantially Compies

2.3. Teaching and Learning Methods

The programme is implemented by use student-oriented teaching and learning methods. Teaching and learning methods correspond to the level of education, course/subject content, learning outcomes, and ensure their achievement.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The Master's Programme in Cybersecurity is implemented using a variety of teaching and learning methods that are generally appropriate to the specificity of the study field and consistent with the intended learning outcomes. The programme integrates lectures, laboratory work, case-based analysis, project-based learning, debates, independent study, and consultation sessions.

Technical courses demonstrate a strong emphasis on laboratory-based instruction, providing students with opportunities to apply cybersecurity tools and methodologies in controlled environments. The Panel observed that the practical components are well integrated into the course structures, particularly in subjects such as Penetration Testing, Malware Analysis, Intrusion Detection, and Cloud Security. These components support the development of applied competencies relevant to contemporary cybersecurity practice.

Courses related to governance, compliance, and data protection demonstrate more student-centered and analytical teaching approaches. These include case studies, structured debates, written policy analysis, and audit simulations. Such methods are appropriate for developing transferable skills, including critical thinking, professional communication, and ethical reasoning.

The teaching methods are aligned with the programme learning outcomes at a structural level.

Here are certain areas where further strengthening is advisable: The practical exercises are well developed, in several technical courses the instructional approach appears predominantly operational. To fully reflect Master-level expectations, teaching methods should more consistently incorporate analytical synthesis, comparative evaluation of methodologies, and innovation-driven assignments. The integration of research-informed tasks within technical subjects would enhance the academic depth of instruction. The progression of complexity across the curriculum could be articulated more explicitly.

Evidences/Indicators

- Component evidences/indicators, including the relevant documents and interview results

Recommendations:

Suggestions for the Programme Development

- Strengthen integration of research-based and analytical tasks within technical courses to better reflect Master-level expectations.
- Introduce advanced integrative projects requiring synthesis of multiple cybersecurity domains.
- Encourage greater incorporation of comparative analysis of tools, frameworks, and methodologies within technical coursework

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
2.3. Teaching and learning methods	Complies

2.4. Student Evaluation

Student evaluation is conducted in accordance with the established procedures. It is transparent, reliable and complies with existing legislation.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

Student evaluation within the Master's Programme in Cybersecurity is conducted in accordance with national legislation and institutional regulations. The grading system follows the Order of the Minister of Education and Science of Georgia and applies a 100-point scale with clearly defined positive and negative grade ranges. The minimum passing thresholds for midterm and final assessments are explicitly defined in programme documentation. Course syllabi specify assessment forms, grading criteria, weighting of components, and minimum competence requirements. Students are informed of evaluation criteria at the beginning of each course. The assessment structure includes ongoing assessment, midterm examinations, final examinations, laboratory work, written assignments, and thesis defense. The programme defines transparent grading categories (A–F scale) and clearly regulates procedures for additional examinations and appeals. Students receiving an FX grade are granted the right to an additional examination in accordance with established procedures. Appeal mechanisms are described and align with institutional policies. The evaluation of the Master's thesis is regulated through a formal defense procedure conducted by an examination commission consisting of 5–7 members. The thesis is assessed using predefined criteria including research relevance, literature review, methodological application, result analysis, conclusions, and presentation quality. The evaluation process includes documented protocols. The programme also implements an outcome-based assessment framework using performance indicators and rubric-based scoring. While the operationalization of the 1–2–3 outcome mapping requires further methodological clarification for internal quality assurance purposes, the grading of individual students is conducted through clearly defined, syllabus-based assessment criteria.

Evidences/Indicators

- Component evidences/indicators, including the relevant documents and interview results

Recommendations:

- Proposal (s), which should be considered by the HEI, the programme to meet the requirements of the standard

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
2.4. Student evaluation	Complies

3. Student Achievements, Individual Work with Them

The programme ensures the creation of a student-centered environment by providing students with relevant services; promotes maximum student awareness, implements a variety of activities and facilitates student involvement in local and/or international projects; proper quality of scientific guidance is provided for master's student.

3.1 Student Consulting and Support Services

Students receive consultation and support regarding the planning of learning process, improvement of academic achievement, and career development from the people involved in the programme and/or structural units of the HEI. A student has an opportunity to have a diverse learning process and receive relevant information and recommendations from those involved in the programme.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

Within the framework of the evaluation of the joint Master's Program in Cybersecurity implemented by Georgian Technical University and the British University, the panel examined the student support mechanisms developed by both institutions. Given that the program is new and does not yet have students with active status, interviews were conducted

with students and graduates of other ongoing programs at Georgian Technical University and the British University.

The interviews, along with the analysis of documentation and university websites, demonstrated that students of both universities benefit from a wide range of support services. In the event of accreditation of the Master's program in Cybersecurity, students enrolled in the program will have access to the full spectrum of activities and services offered by both institutions.

During the interviews, students and graduates noted that at the beginning of their studies they attend orientation meetings, where university representatives introduce them to various student services and explain issues related to the administration of the academic process. Employment contracts with academic staff and course syllabi include consultation hours, during which students receive essential and relevant information. In addition, regular meetings are held concerning the use of library resources, career development opportunities, and exchange programs. Also, Students have the opportunity to take advantage of consulting hours from both universities. The interview findings indicate that the staff of both universities demonstrate a strong commitment to addressing student needs. Particular attention should be given to the "Mentorship System" implemented by the British University. Upon enrollment, each student is assigned a personal mentor with whom they hold regular meetings to discuss matters such as career development, personal interests, selection of conference topics, problem-solving strategies, and related issues. Students of the British University emphasized the importance of this system during interviews and assessed their experience positively. Both the British University and Georgian Technical University actively promote high-quality integration of students into the academic process. Student self-governance bodies operate at both institutions and are actively involved in students' daily activities. Various sports clubs are also available, enabling students to participate in activities aligned with their individual interests. In addition to these activities, the universities offer diverse opportunities for participation in international exchange programs. During the interviews, students and graduates indicated that they had participated in exchange programs in Japan, the United Kingdom, Budapest, Italy, Austria, and other countries. Students are informed about exchange

opportunities through various platforms, which they use effectively. Students are actively involved in grant-funded and research projects such as Erasmus+, Horizon, NATO initiatives, and projects funded by the Shota Rustaveli National Science Foundation of Georgia, among others. They also participate in conferences, and their academic papers are published in various scientific journals. Furthermore, students reported that they regularly receive information about employment and career development opportunities via notifications and email communication.

At the British University, the Vazha-Pshavela Foundation operates to support student initiatives, provide financial assistance for tuition, and facilitate participation in various activities. In the 2023–2024 academic year, at the initiative of British University students, the magazine "BUG Tells" was established. Both the visual and substantive components of the magazine are created entirely by students. When necessary, they receive support from the Student and Alumni Relations Office as well as from the Public Relations Department. Based on the analysis of the presented documentation and interview results, it can be concluded that, in the event of the implementation of the Master's Program in Cybersecurity, the universities will be able to provide their students with comprehensive and diverse support services.

Evidences/Indicators

- Implementation Guide (Draft) for the Joint Master's Program in Cybersecurity
- Student participation in grant programs
- Statistics on student participation in conferences
- Published student articles
- Exchange program participation statistics
- Memoranda with international universities
- Memoranda with employers
- Agreement on the implementation of the joint educational program
- Statute of the Student and Alumni Relations Office
- Memoranda of cooperation with employers and international partners
- Statute of the GTU Student Self-Government
- Statute of the GTU Department of Sports, Culture, and Student and Alumni Relations
- Career Development Department activities
- Academic staff contract template

- University websites
- Interview results

Recommendations:

- Proposal (s), which should be considered by the HEI, the programme to meet the requirements of the standard

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
3.1 Student Consulting and Support Services	Complies

3.2. Master's Student Supervision

- A scientific supervisor provides proper support to master's student to perform the scientific-research component successfully.
- Within master's programmes, ration of students and supervisors enables to perform scientific supervision properly.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

Based on the documentation and interviews presented during the evaluation process of the joint Master's Program in Cybersecurity implemented by Georgian Technical University and the British University, it should be noted that the institutions operate in accordance with the regulatory documents developed by Georgian Technical University. According to the Regulations on Master's Studies of Georgian Technical University, a Master's thesis supervisor may be a Professor, Associate Professor, Assistant Professor, invited academic staff member/lecturer holding a doctoral degree, Professor Emeritus, or a Chief or Senior

Researcher holding a doctoral degree affiliated with a scientific institute or center integrated with GTU. A thesis supervisor may also be a doctoral degree holder from another institution, provided that a relevant agreement or memorandum exists between GTU and the respective institution. To facilitate the selection of a thesis topic and supervisor for newly enrolled Master's students, the Head of the Academic Department organizes meetings between students and potential supervisors. Supervisors present tentative thesis titles, explain their relevance, and outline their research directions. Students have the right to propose topics of personal interest. Based on these meetings, students make their selection and submit a formal application to the Head of the Academic Department. Alternatively, students may select a topic and supervisor from the list published on the faculty website and apply without attending the meeting. Following departmental review, the Head of the Academic Department submits the list of selected supervisors and thesis topics to the Dean's Office, accompanied by the relevant documentation. According to the draft Implementation Guide for the Joint Master's Program in Cybersecurity, supervision within the joint program framework is conducted with the participation of at least two supervisors jointly appointed by the partner universities (one supervisor from GTU, the other supervisor from a British university). This model ensures alignment of academic standards, interdisciplinary relevance of the thesis topic, and unified oversight of research quality.

The thesis topic and supervisor are approved during the first semester, in accordance with the academic calendar. Approval procedures are carried out in compliance with jointly agreed regulations and involve the program directors and relevant academic structural units of the partner institutions. The thesis defense is conducted before a joint defense committee composed of representatives from both partner universities. The composition of the committee and defense procedures are approved by a decision of the Governing Board.

Although the draft guide does not specify the exact rights and responsibilities of the scientific supervisor, the GTU Master's Regulations stipulate that the supervisor is obliged to oversee the thesis process, provide consultations regarding literature search and review, methodology development, analysis of results, preparation of a work plan and schedule, defense procedures, and all other necessary matters. During interviews, students and graduates of both universities

indicated that they had continuous consultation meetings with their supervisors and encountered no difficulties in this regard. It should also be noted that neither the GTU Master's Regulations nor the draft Implementation Guide for the joint program provide specific information regarding the methodology for determining the ratio of students to supervisors.

During interviews, program directors and representatives of the Quality Assurance Service stated that a scientific supervisor is permitted to supervise up to two Master's students with active status simultaneously, which is also confirmed by academic staff contract templates. The universities also presented information on prospective supervisors for the joint program, indicating that 10 GTU academic staff members are considered as potential supervisors, 2 of whom do not hold a doctoral degree. In order to ensure effective supervision within the joint Master's Program, it is recommended that a specific regulation for joint Master's programs be developed. This regulation should clearly define the procedures for the selection, appointment, and replacement of supervisors/co-supervisors, outline their rights and responsibilities, establish the methodology for determining the supervisor-to-student ratio, and regulate all other relevant aspects.

Interviews further revealed that the institutions continuously work on mechanisms for evaluating the quality of thesis supervision, thereby ensuring the effective implementation and further development of the supervision process. This is supported by the results of student and graduate surveys, as well as by research findings presented by the universities.

Data related to the supervision of master's students	
Number of master theses supervisors	10
Number of master's students	50
Ratio - supervisors of master's theses/master's students	0,2

Evidences/Indicators

- Regulations on Master's Studies of Georgian Technical University
- Instruction for Formatting a Master's Thesis
- Draft Implementation Guide for the Joint Master's Program in Cybersecurity (LEPL Georgian Technical University and Ltd. British University)
- Research Component Evaluation – Semester Survey Report for Master's and Doctoral Students
- Academic staff CVs
- Staff implementing the English-language Master's Educational Program in Cybersecurity
- Interview results

Recommendations:

- It is recommended to develop a specific regulation for the joint Master's Program that comprehensively defines the procedures for the selection, appointment, and replacement of supervisors/co-supervisors, clarifies their rights and responsibilities, establishes a transparent methodology for determining the supervisor-to-student ratio, and regulates all other relevant aspects necessary for the effective implementation of the program.

- o Define supervisor workload limits and supervisor-to-student ratio

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
3.2. Master's Students Supervision	Substantially Compies

4. Providing Teaching Resources

Human, material, information and financial resources of educational programme ensure

sustainable, stable, efficient and effective functioning of the programme and the achievement of the defined objectives.

4.1 Human Resources

➢ Programme staff consists of qualified persons, who have necessary competences in order to help students to achieve the programme learning outcomes.
➢ The number and workload of programme academic/scientific and invited staff ensures the sustainable running of the educational process and also, proper execution of their research/creative/performance activities and other assigned duties. Quantitative indicators related to academic/scientific/invited staff ensure programme sustainability.
➢ The Head of the Programme possesses necessary knowledge and experience required for programme elaboration, and also the appropriate competences in the field of study of the programme. He/she is personally involved in programme implementation.
➢ Programme students are provided with an adequate number of administrative and support staff of appropriate competence.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The program is implemented by qualified academic and invited staff, including 8 professors, 2 associate professors, and 4 Assistant Professors. The university has established specific regulations for recruiting academic personnel for different positions, clearly defining their rights, responsibilities, and evaluation procedures. According to the regulations adopted by both partner universities, the performance of academic and invited staff is evaluated annually. This evaluation determines their teaching and research responsibilities in accordance with their academic position and contractual obligations.

The duties of academic and invited staff include active participation in the development and continuous improvement of the program, as well as providing student consultation and academic support. These responsibilities are regulated by institutional policies and formal employment contracts.

The program also involves 2 associate professors, 1 assistant professor, and 1 professor from the British University, all affiliated with their respective institution. From Georgian Technical University, 10 representatives participate in the program: 7 professors and 3 assistant professors, all formally affiliated with the university.

The heads of the program coordinate the development and improvement processes through established internal quality assurance mechanisms. Their responsibilities are defined in official contracts and approved by the university administration. The workload of academic and invited staff is calculated in accordance with the institutional workload regulation. The calculation takes into account teaching hours, research activities, and other academic responsibilities. In addition, the institution considers staff members' academic workload at

other higher education institutions to ensure that the overall workload remains balanced and compatible with the effective implementation of the educational program.

The Program Head of the Artificial Intelligence Department at Georgian Technical University, holds a Candidate of Technical Sciences degree and is currently a PhD student in Educational Sciences. She is the author of more than 40 scientific publications and 4 books and has completed professional development activities at the University of Magdeburg (2021) and the University of Saarbrücken (2022). The Co-Head of the Program is a professor and Head of the Information Technology Department at Georgian Technical University. He holds a Candidate of Technical Sciences degree and is the author of approximately 100 scientific papers and 14 books.

Overall, the academic and invited staff have scientific and teaching capacity, and their number and workload ensure the successful implementation of the educational program and effective management of the teaching process. However, an area identified for further improvement concerns the strengthening of academic qualifications and expertise specifically in the field of Cybersecurity. While the program benefits from a solid academic foundation in related technological fields, the current staff composition indicates a limited number of faculty members with specialized theoretical and practical experience in cybersecurity. Given the strategic importance and rapidly evolving nature of this field, it is suggested that the program be supported by academic personnel who possess in-depth theoretical knowledge, active research engagement, and practical experience in cybersecurity, including participation in relevant projects, applied research, and collaboration with industry.

In addition, the research potential of assistant and associate professors, particularly in cybersecurity-related topics, suggests further enhancement. Increasing their scientific publications, research activities, and involvement in international collaborations would significantly contribute to strengthening the program's academic profile and ensuring its long-term competitiveness and alignment with labor market demands.

Number of the staff involved in the programme (including academic, scientific, and invited staff)	Number of Programme Staff	Including the staff with sectoral expertise[5]	Including the staff holding PhD degree in the sectoral direction[6]	Among them, the affiliated staff
Total number of academic staff	14	14	8	14
- Professor	8	8	8	8
- Associate Professor	2	2	1	2
- Assistant-Professor	4	4	4	4
- Assistant	0	0	0	0
Visiting Staff	0	0	0	0
Scientific Staff	8	0	0	0
Including International Stuff	1	1	1	0

Evidences/Indicators

- Self-evaluation report;
- Unified rule for hiring academic staff at Georgian Technical University;
- Staff documentation;
- Program documentation;
- Contracts ;
- Interview results;

Recommendations:

Suggestions for the Programme Development

- The universities may improve the qualifications of academic staff in cybersecurity by involving and developing specialists who have both strong theoretical knowledge and practical experience in this field.

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation

[5] Staff implementing the relevant components of the main field of study
[6] Staff with relevant doctoral degrees implementing the components of the main field of study

4.1 Human Resources	Complies

4.2 Qualification of Supervisors of Master's Students

The Master's students have qualified supervisor/supervisors and, if necessary, co-supervisor/co-supervisors who have relevant scientific-research experience in the field of research.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

Each master's student is assigned a qualified supervisor with relevant research experience in the technology field. Georgian Technical University regulations clearly define the rights and responsibilities of supervisors. Supervisors may be professors, associate professors, assistant professors, invited lecturers holding a PhD degree, emeritus professors, or senior researchers from scientific institutes affiliated with the university. A supervisor may also represent another institution if a formal agreement exists between the parties.

At the beginning of the study process, the supervisor and the student jointly develop an individual study and research plan, which includes the title of the master's thesis, selected courses, and planned research activities. The supervisor provides continuous academic guidance throughout the research process and supports the student in preparing the thesis for defense.

To facilitate the selection of a research topic and supervisor, the department organizes meetings with potential supervisors. During these meetings, academic staff present proposed research topics, explain their relevance, and introduce their research interests. Students may also propose their own research ideas. After making a decision, students formally apply to the Head of the Department. Additionally, they may select a topic and supervisor from the list published on the faculty's official website. Students are entitled to change their supervisor or appoint a co-supervisor when necessary.

Supervisors guide students in conducting research and preparing their master's theses, while also supporting their integration into local and international research communities. They assist students in preparing scientific articles for publication in peer-reviewed journals and encourage participation in academic conferences and research events. The academic staff involved in the program demonstrate active engagement in research activities across various fields of Information and Communication Technologies over the past five years.

Within the framework of this program, the current number of academic staff eligible to supervise master's theses raises concerns regarding capacity. The program plans to enroll 50 students, while only 10 academic staff members are authorized to supervise master's theses. According to information obtained during interviews, each academic staff member can

supervise a maximum of two master's students. Consequently, the existing supervisory capacity allows for the supervision of only 20 students, which is significantly lower than the planned intake. Therefore, the number of qualified scientific staff to meet the projected demand is suggested to be increased, particularly in the field of cybersecurity, where specialized expertise is especially important for the program's development.

It is also important to note that out of the 10 academic staff members qualified to supervise master's theses, only 8 hold a PhD degree. Considering the academic level of the program and the planned student intake, it is suggested to increase the proportion of staff holding a PhD degree in order to ensure stronger research supervision and maintain academic standards.

Number of supervisors of Master's theses	**Thesis supervisors**	**Including the supervisors holding PhD degree in the sectoral direction**	**Among them, the affiliated staff**
Number of supervisors of Master's thesis	10	7	7
- Professor	7	7	7
- Associate Professor	1	1	1
- Assistant-Professor	2	2	2
Visiting personnel	0	0	0
Scientific Staff	8	7	7

Evidences/Indicators

- Self-evaluation;
- Course Instructors;
- Staff Documentation;
- Master's Program Regulation;
- Interview results;

Recommendations:

-

Suggestions for the Programme Development

- The universities may increase the number of qualified academic staff eligible to supervise master's theses, particularly in cybersecurity, and strengthen the involvement of personnel holding doctoral degrees to ensure adequate supervision capacity for the planned student enrollment.

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
4.2 Qualification of Supervisors of Master's Students	Complies

4.3 Professional Development of Academic, Scientific and Invited Staff

➢ The HEI conducts the evaluation of programme staff and analyses evaluation results on a regular basis.
➢ The HEI fosters professional development of the academic, scientific and invited staff. Moreover, it fosters their scientific and research work.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The universities have implemented a mechanism for evaluating the performance of academic and invited staff, which includes both semester-based and annual evaluations. At Georgian Technical University, staff performance evaluation is based on an annual scientific reporting system, faculty-level reviews, and assessments of professional and research potential.

To support professional development, both universities implement a wide range of activities, including training in modern teaching and learning methodologies, assessment systems, academic integrity, and the use of Artificial Intelligence in education. Georgian Technical University operates a Professional Development Center aimed at strengthening staff competencies, while the British university promotes teaching quality through international partnerships and experience-sharing seminars. Academic staff participate in international conferences, mobility programs (including Erasmus+), partnership events, and masterclasses.

In order to further strengthen the program's profile, it is important to place greater emphasis on expanding academic and research activities specifically in the field of Cybersecurity. This includes increasing the number of publications in high-impact, peer-reviewed journals dedicated to cybersecurity, enhancing participation in specialized international conferences and scientific forums in this field, promoting academic mobility and research exchanges focused on cybersecurity topics, and organizing targeted workshops, seminars, and training sessions addressing current challenges such as cyber defense, data protection, and information security management. Strengthening collaboration with international research centers, industry partners, and cybersecurity laboratories would also contribute to integrating practical expertise with academic research and increasing the visibility and impact of research outcomes in this strategic domain.

The British University has established the Advance Research and Policy Development Institute, which administers internal grant competitions, develops individual research plans for staff members, and monitors their implementation. The university also operates an internal grant funding scheme that promotes the involvement of both academic staff and students in research activities. At Georgian Technical University, the necessary material and technical infrastructure has been developed, including research institutes, laboratories, and libraries, providing an appropriate environment for conducting research and expanding field-specific initiatives, including those in cybersecurity.

International cooperation remains a key strategic priority for both universities. Collaboration with foreign universities and organizations includes exchange programs, joint research projects, and the co-organization of international conferences. Expanding these partnerships with a stronger focus on cybersecurity-related research networks, joint publications, and thematic events will further enhance internationalization and strengthen the global recognition of research outcomes in this field.

Overall, the existing mechanisms ensure a systematic approach to staff performance evaluation, continuous professional development, research capacity building, and international integration. At the same time, increasing targeted academic and research activities in cybersecurity will further improve program quality, reinforce its strategic orientation, and support the professional growth of academic staff in this rapidly evolving and high-demand field.

Evidences/Indicators

- Self-evaluation;
- Course Instructors;
- Staff Documentation;

- Educational Program;
- Interview results;

Recommendations:

- N/A

Suggestions for the Programme Development

- It is suggested to strengthen academic and research activities in the field of cybersecurity within the program, including increasing the number of publications in international peer-reviewed journals, enhancing participation in specialized conferences, expanding academic mobility, and organizing targeted workshops and training sessions.
- It is suggested to increase field-specific activities at the British university.

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
4.3 Professional development of academic, scientific and invited staff	Complies

4.4. Material Resources

Programme is provided by necessary infrastructure, information resources relevant to the field of study and technical equipment required for achieving programme learning outcomes.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

Both partner universities confirm and undertake the obligation to fully meet the material and technical resource requirements necessary for the implementation of the program. At the British University, the library fund is equipped with program-required literature in both printed and electronic formats (approximately 1,200 resources). The university provides an electronic catalog, a reading hall, a book reservation service, and interlibrary loan services.

Students and staff have access to international scientific databases (including Cambridge, SAGE, Edward Elgar, and others), as well as the Learning Management System (Canvas). The university is supported by modern infrastructure, including appropriate academic and administrative spaces, IT infrastructure, and safety systems.

Georgian Technical University's material and technical base quantitatively and qualitatively ensures the achievement of the program's objectives and learning outcomes. The university operates modern laboratories, including 19 teaching and research laboratories and 16 computer labs (340 workstations), specialized research institutes, FabLab, and internationally accredited laboratories. The university library provides access to more than 150,000 digitized resources and international databases (including Elsevier and others). Within the framework of the partnership, a modern Artificial Intelligence and Cybersecurity laboratory has been established, technical equipment has been upgraded, and academic and research resources from international publishers have been acquired.

Overall, the existing infrastructure and resources ensure the effective implementation of teaching and research processes, support the development of students' practical and research skills, and contribute to the high-quality delivery of the program.

Evidences/Indicators

- Self-evaluation;
- Educational Program;
- Library, material, information, and digital resources and documents confirming their ownership/license purchase;
- Indicators of the use of access to international electronic library databases;
- Interview results;

Recommendations:

- N/A

Suggestions for the Programme Development

- N/A

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
4.4 Material Resources	Complies

4.5 Programme/Faculty/School Budget and Programme Financial Sustainability

The allocation of financial resources stipulated in the programme/faculty/school budget is economically feasible and corresponds to the programme needs.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The programme budget is compiled according to the Policy for Financial Management and Control at British University. The budget is prepared for 2 years, considering the number of optimal intakes per year - 30 Georgian and 20 international students.

Therefore, the estimated budget of 1 065 000 GEL derives from program revenue. In case of not receiving sufficient number of students for break even, BU ensures allocation of reserve funds to ensure implementation of the program with fewer students.

The programme budget includes direct and indirect expenses. The direct expenses include the salary for academic and invited staff and other related teaching costs - 110 664 GEL in total, funds allocated for CISSP exam (150 000 GEL) and for teaching materials (30 000). The rest of the expenses include internationalization (45 000 GEL) and research and development funds (30 000 GEL). Programme accreditation and other indirect expenses are also envisaged by the budget. Overall, for 50 students per cohort, the programme budget seems to be profitable, estimated at 637 082 GEL.

Considering all above mentioned, allocation of financial resources stipulated in the programme budget is economically feasible and corresponds to the programme needs and requirements. Reserved funds ensure programme sustainability and development.

Evidences/Indicators

- The Self-evaluation report
- The programme budget
- Interview results

Recommendations:

- Proposal (s), which should be considered by the HEI, the programme to meet the requirements of the standard

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
4.5. Programme/ Faculty/School Budget and Programme Financial Sustainability	Complies

5. Teaching Quality Enhancement Opportunities

In order to enhance teaching quality, programme utilises internal and external quality assurance services and also, periodically conducts programme monitoring and programme review. Relevant data is collected, analysed and utilized for informed decision making and programme development.

5.1 Internal Quality Evaluation

Programme staff collaborates with internal quality assurance department(s)/staff available at the HEI when planning the process of programme quality assurance, developing assessment instruments, and implementing assessment process. Programme staff utilizes quality assurance results for programme improvement.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The Master's Program in Cybersecurity is jointly administered by BU and GTU, therefore, programme quality assessment is streamlined by an inter-institutional quality assurance approach defined by the agreement for program implementation.

The Internal Quality Assurance mechanisms at British University in Georgia are defined and regulated by the "Quality Assurance Mechanisms" which includes: evaluation of educational programmes and teaching-learning quality, evaluation of services and resources, evaluation of staff implementing the programme, evaluation of research and other activities, evaluation of the effectiveness of organizational management, evaluation of the contribution made by the university for the development of society. Besides, Internal Quality Assurance mechanisms at GTU are defined by the regulation of the Quality Assurance Office. Internal quality assurance includes the systemic evaluation of teaching and scientific-research activities, evaluations of curricula, services, and resources, assessment of quality of the professional development and facilitates continuous improvement through recommendations and findings.

In relation to educational programme, both universities have developed a rule for planning, developing, amending and canceling educational programmes, which defines evaluation tools, assessment area and periodicity. The same approach is elaborated by institutions concerning all evaluation mechanisms of internal quality assurance. Educational programmes are subject to periodic monitoring/evaluation. Therefore, internal quality assurance includes the systemic surveys and evaluations of curricula, services, and resources.

Program quality assurance is based on the PDCA - "plan –do – check -act" principle. The process implies the involvement of all interested parties in the process of development of educational activities and capacity of the programme, as both institutions prioritize students, graduates, employers, academic and invited staff involvement in the internal quality assessment process.

In accordance with the evaluation of the submitted documents and accreditation visit findings, the accreditation panel finds that programme evaluation is consistent and assessment results are generally utilised for programme improvement. The QA representatives cooperate with the programme staff and ensure the evaluation process is constructive, therefore, a Self-Evaluation Report of the programme is prepared with the involvement of academic and administrative staff and other relevant stakeholders from both institutions.

As the program does not have students and alumni yet, it can be confirmed that students and alumni from other related programs have been involved in the self-evaluation process. Necessity-based and need assessment surveys are used by internal quality evaluation processes for purposely identifying the problems and ensuring quality improvement interventions. These surveys are targeted to identify the satisfaction, needs, and wants of the students, as well as annual students and staff satisfaction surveys, are conducted for assessing the general administration of the programmes and availability of services.

At the end of each academic year, HEIs are introducing findings and results of internal quality assessment loops to the Governing Board, that discusses the reports from each institution and extends recommendations if relevant.

Evidences/Indicators

- Self-Evaluation Report
- Quality Assurance Mechanisms for both HEIs
- Rules and procedures for planning, developing, approving, amending and canceling educational programs
- Agreement concerning implementation of the programme
- Survey forms and results
- Interview results

Recommendations:

- Proposal (s), which should be considered by the HEI, the programme to meet the requirements of the standard

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
5.1 Internal quality evaluation	Complies

5.2 External Quality Evaluation

Programme utilises the results of external quality assurance on a regular basis.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

External quality assurance at GTU and BU is mainly carried out through Accreditation and Authorization processes, maintained by the National Center for Educational Quality Enhancement. The quality assurance service at each institution reviews recommendations and suggestions and the findings are introduced to the heads of the programmes for further consideration. Therefore, the QA Office ensures compliance of the developments with the received recommendations.

Institutions also actively utilize developmental peer evaluation for the programme development and improvement. The Cybersecurity educational programme was evaluated by the Professor in Computer Engineering at Ilia State University. The evaluation highlighted the importance and individualism of the program, alignment of program goals with contemporary tendencies and labor market requirements, peculiarities of the curricula and research.

Evidences/Indicators

- Self-Evaluation Report
- Quality Assurance Mechanisms for both HEIs
- Agreement concerning implementation of the programme
- Survey reports and forms
- Benchmark of analogue programs

- Interview results

Recommendations:

- Proposal (s), which should be considered by the HEI, the programme to meet the requirements of the standard

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
5.2. External Quality Evaluation	Complies

5.3 Programme Monitoring and Periodic Review

Programme monitoring and periodic evaluation is conducted with the involvement of academic, scientific, invited, administrative, supporting staff, students, graduates, employers and other stakeholders through systematic data collection, study and analysis. Evaluation results are applied for the programme improvement.

Summary and Analysis of the Education Programme's Compliance with the Requirements of the Component of the Standard

The fact that the programme quality assessment is streamlined by an inter-institutional quality assurance approach defined by the agreement for program implementation, ensures constant cooperation and joint contribution to the quality enhancement at the programme level. For program development and service improvement, the QA Office at British University and Georgian Technical University ensure monitoring and periodic assessment. The assessment and evaluation process involves internal and external stakeholders. Surveys with staff, students, and employers are central tools for implementing monitoring of the educational

programs of the university. At the end of every compulsory course, students evaluate the course by completing a course evaluation form, in case of necessity focus groups are also organised. Satisfaction and need assessment surveys are used to identify improvements and priorities, to ensure an effective monitoring process. Master students are also evaluating the process of supervision and effectiveness of supervisors. Results of the evaluation process are distributed among the programme team and are used for the programme improvements.

The programme also benefits from the practice of classroom observation, when evaluations are conducted with peers, as well as quality assurance service representatives with predetermined periodicity and procedure. The collegial attendance team prepares the mutual attendance schedule and teaching and learning evaluation criteria/indicators, through which the lecture/practical teaching is evaluated.

At the end of each semester, the Quality Assurance Offices monitor the students' academic performance, and the evaluation results are used by the university administration, shared with the Governing Board and discussed together to improve educational processes. The institutions have practice to assess the programme efficiency – the periodic internal self-evaluation of the educational programs of the university. The process includes drafting a self-evaluation report of the educational programmes, with the aim of identifying strengths and areas for improvement. Periodic self-evaluation of the programmes includes following components: analysis of students academic performance, semester survey of students regarding courses/program components, evaluation of invited and academic staff involved in the program based on student surveys, and evaluations of employers and external experts.

For continuous development and identifying tendencies, the reports are evaluated in accordance with the dynamics, self-assessment process findings are compared with ones in each subsequent reporting period. Evaluation is oriented at identifying the causes of deviations (if existent) and implementing measures to eliminate them - making certain changes within the program and/or course; modifying the teaching and learning methods; optimising the evaluation methods used within the syllabus of the training course; changing the literature used within the training course; establishing/changing the prerequisites of the training course and etc.

The HEIs ensure benchmarking for the best available practices to develop a competitive and individual programme. The programme takes into consideration the experiences of the leading universities in the field - Carnegie Mellon University – MS in Information Security (MSIS), Carnegie Mellon University – MS in Information Security (MSIS), University of Warwick – MSc Cyber Security Management, SANS Technology Institute – MS in Information Security Engineering (MSISE), University of Warwick – MSc Cyber Security and Management (WBS/WMG). Many common courses and research peculiarities have been observed that affected the elaboration process of the program, but also considers local Georgian realities and demands, therefore, incorporates both, local and international practices and requirements.

Evidences/Indicators

- Self-Evaluation Report
- Quality Assurance Mechanisms for both HEIs
- Rules and procedures for planning, developing, approving, amending and canceling educational programs
- Agreement concerning implementation of the programme
- Survey forms and results
- Interview results

Recommendations:

- Proposal (s), which should be considered by the HEI, the programme to meet the requirements of the standard

Suggestions for the Programme Development

- Non-binding suggestions for programme development

Evaluation

Please, evaluate the compliance of the programme with the component

Component	Evaluation
5.3. Programme monitoring and periodic review	Complies

Attached documentation (if applicable):

Signatures:

Chair of Accreditation Expert Panel

Seifedine Kadry,

Accreditation Expert Panel Members

Magda Tsintsadze

Lia Kurtanidze

Tamta Tskhovrebadze, signature

Tamar Tkhelidze