Study Programme “Security and Personal Data Protection” Self-Assessment

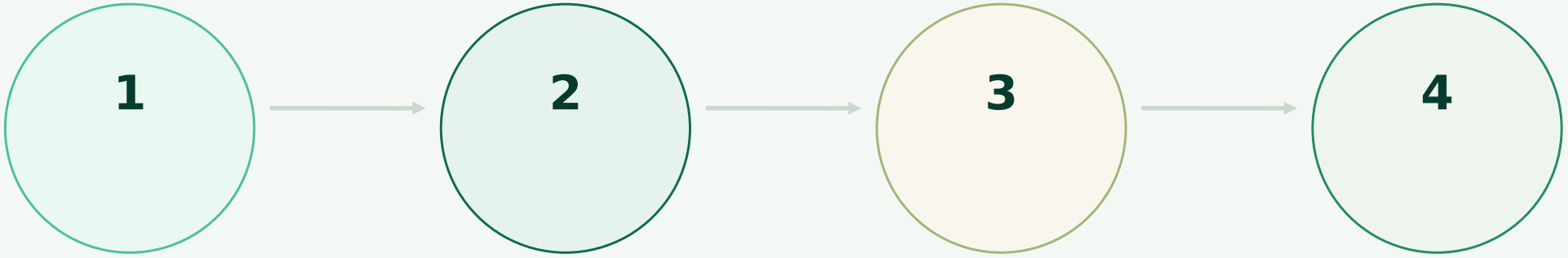
2025 academic year

Self-assessment as a tool for evaluating the programme’s relevance, quality and development directions.

Approved: at the Council meeting, Minutes No. 2-01/136, 26.03.2026

What does the self-assessment evaluate?

The programme’s alignment with industry trends, regulation and the quality principles of professional higher education.



Relevance

Economic and social rationale

Implementation

Content, methods, practical training and results

Demand

Admissions, graduates and labour market

Development

SWOT analysis and future directions

Main idea: the programme is viewed as an integrated professional training system, not merely as a set of study courses.

Source: study programme self-assessment document

Why is the programme needed?

Security and personal data protection competence is becoming a horizontal requirement for organisations.

Regulation

GDPR • NIS2 • DORA • National Cybersecurity Law • Cabinet Regulation No. 397

Risks

Cyber incidents, data breaches, supply-chain and business-continuity risks

Organisational needs

Need for compliance, risk management, incident reporting and internal control

Specialist

A profile that connects law, technical foundations, risks and governance

Social value

Protection of individual rights, resilience of essential services and trust in the digital environment.

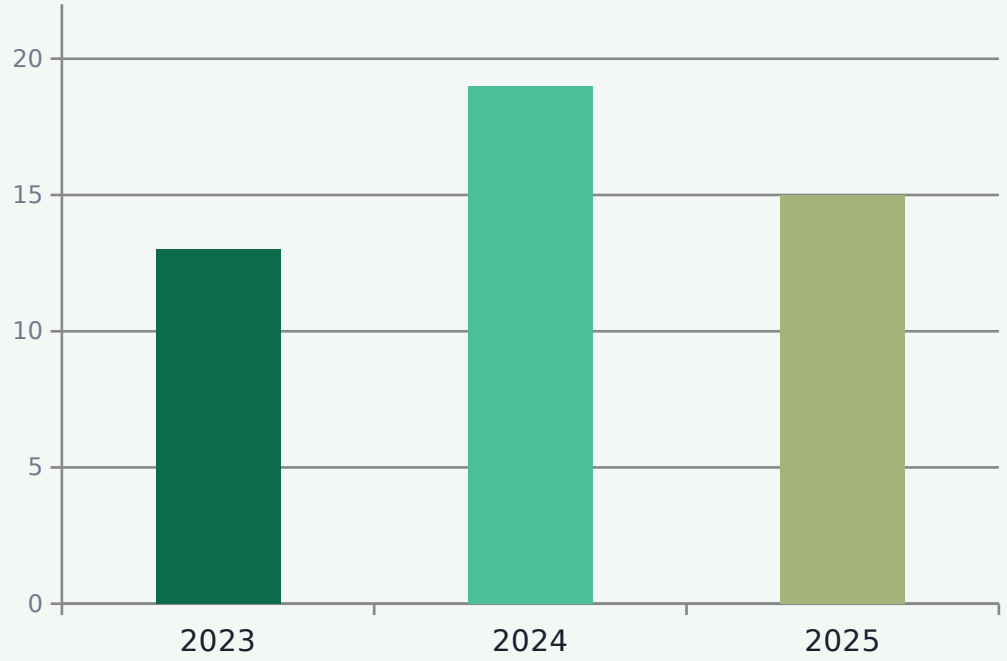
Economic value

Lower risk of incidents and downtime, higher compliance and stronger organisational security capability.

Source: study programme self-assessment document

Admissions dynamics: a stable professional niche

In 2023–2025, demand fluctuates but remains above the initial level.



INTERPRETATION

- In 2024, growth of +46.2% compared with 2023.
- In 2025, a decrease to 15, while the level still exceeds 2023.
- The programme most strongly appeals to working professionals and people with clear career motivation.

MODE OF DELIVERY

Demand is concentrated in flexible modes: extramural and part-time on-site studies. This matches the target audience, which combines studies with work.

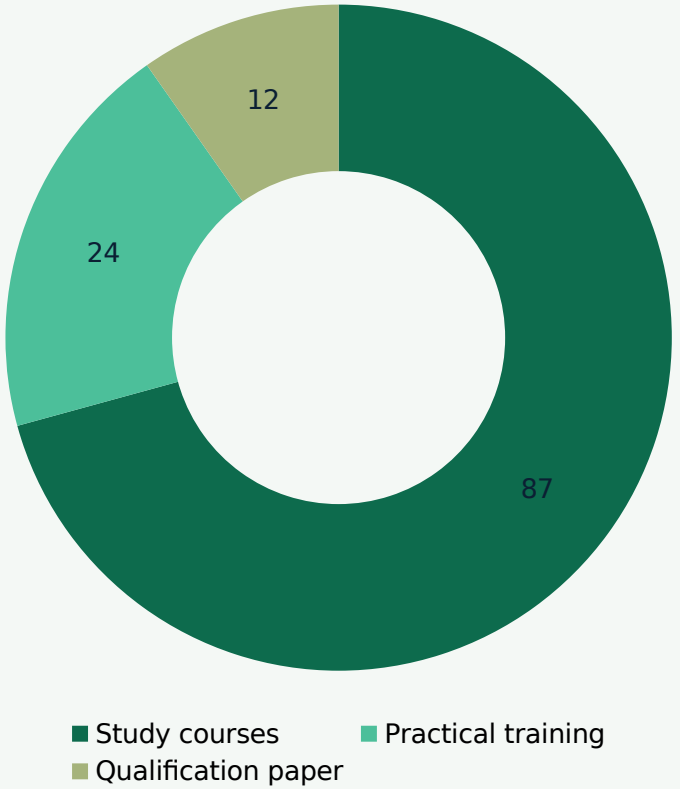
Key conclusion

Not a mass-market programme, but a professionally oriented offer with a clearly defined audience.

Source: study programme self-assessment document

Programme structure: 123 credit points

The content is designed as sequential competence development from foundations to specialisation, practical training and the qualification paper.



CONTENT LOGIC

Part A

general education foundation

law, language, IT introduction, human security

Part B

professional core

data protection, information security, cybersecurity, risks, incidents

Part C

elective modules

OSINT, Python, offensive tools, psychology, mediation

Training + paper

professional validation

24 CP practical training and 12 CP qualification paper

Full-time studies: 4 semesters • Part-time on-site studies: 5 semesters

Source: study programme self-assessment document

Learning outcomes: a broad security specialist profile

The outcomes connect security planning, people management, technical solutions and regulatory compliance.

The set of outcomes develops a professional able to operate at the intersection of organisational security, compliance and data protection.

Source: study programme self-assessment document

Implementation methods: from theory to practical action

Lectures, practical assignments, case analysis and blended learning are combined with transparent assessment.

Up to 50%

remote classes in certain courses according to the schedule

Competence demonstration

assessment includes practical assignments, participation, tests, examinations and presentations

Source: study programme self-assessment document

Practical training: a bridge to the working environment

24 CP practical training is one of the central components of the programme and demonstrates the practical applicability of the outcomes.

CONTENT OF PRACTICAL TRAINING TASKS

IT infrastructure	network topology, servers, devices, services
Vulnerabilities	assessment of perimeter and internal security weaknesses
Laws and regulations	internal documentation, duties, responsibility
Incident management	procedure, logs, notification and recommendations

RESULT

Practical training report with practical information collected, analysis, conclusions and recommendations; assessed by a commission on a 10-point scale.

Source: study programme self-assessment document

Graduate demand: regulation turns into roles

In the labour market, the need is growing for specialists who connect security, compliance, risks and data protection.

GDPR personal data protection

NIS2 cybersecurity governance

DORA digital operational resilience

Cabinet Regulation No. 397 minimum cybersecurity requirements

POSSIBLE JOB ROLES

Security specialist	coordination of organisational security processes
Cybersecurity support specialist	a role explaining risks, incidents and security controls
Compliance / risk coordinator	internal rules, inspections, audit and documentation
Data protection function support	practical implementation of GDPR requirements and employee consultation

Conclusion: the strongest initial competitiveness is expected in junior or mid-level coordination, control and support functions.

Source: study programme self-assessment document

SWOT analysis: programme position in 2025

Strengths and opportunities are significant, but risks related to specialisation, maturity and sector dynamics must be managed.

S Strengths

Interdisciplinarity
Clearly mapped outcomes
Strong practical training component

W Weaknesses

Broad scope may reduce niche depth
Limited reputational momentum of a new programme

O Opportunities

Regulatory demand
Latvia’s digital skills deficit
Linkage with ENISA ECSF

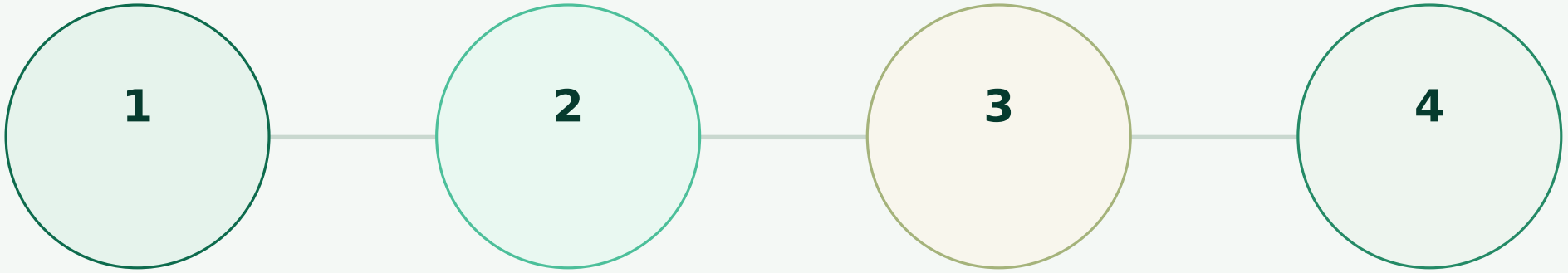
T Threats

Rapid change in the threat environment
Competition from narrow certifications
Limited applicant base

Source: study programme self-assessment document

Strategic development directions

Maintain the interdisciplinary foundation while gradually increasing depth of specialisation and external linkage.



Depth of specialisation

more integrated scenarios, simulations and advanced modules

Industry partnerships

a stable network of practical training placements and employer feedback

Competence mapping

more precise alignment with ENISA ECSF and job-role profiles

Digital pedagogy

systematic evaluation of the impact of blended learning

Priority: position the programme as a practical response to demand for competences in security, data protection and regulatory compliance.

Source: study programme self-assessment document

Closing conclusion

The programme is relevant, socially significant and aligned with the labour market. Its development potential is based on regulatory demand, practical orientation and an interdisciplinary set of competences.

01 Relevance

security and data protection are a horizontal organisational requirement

02 Content alignment

balance of legal, governance and technical foundations

03 Practicality

24 CP practical training strengthens professional readiness

04 Going forward

specialisation, partnerships and competence mapping should be strengthened

Source: study programme self-assessment document