



ASIIN Certification Report

**21 Modules of the
*ONLINE Joint Degree programme
Cybersecurity Management and Data Sovereignty***

Provided by

**German University of Digital Science (UDS), Germany
(Coordinating and certificate-issuing institution)
Munster Technological University (MTU), Ireland
Universidad Internacional de la Rioja (UNIR), Spain**

Version: 16 December 2025 / final version

Table of Content

A About the Certification Process	3
B Characteristics of the Modules	5
C Preliminary Note on the Procedure.....	6
D Expert Report for the ASIIN Certificate	8
1. Content, Structure and Implementation	8
2. Examination: System, Policy and Implementation	15
3. Resources: Staff and Infrastructure	18
4. Quality Management: Monitoring and Continuous Improvement	20
5. Documentation and Transparency.....	22
E Additional Documents	26
F Comment of the Provider (24.11.2025)	27
G Summary: Peer recommendations (04.12.2025)	28
H Decision of the Certification Commission (16.12.2025)	30

A About the Certification Process

Modules	Previous certification
<ol style="list-style-type: none"> 1. Communication Design for Cybersecurity 2. Business Resilience, Incident Management & Threat Response 3. AI & Emerging Topics in Cybersecurity 4. Cybersecurity Culture, Strategy & Leadership 5. Enterprise Architecture, Infrastructure Design and Cloud Computing 6. Law, Compliance, Governance, Policy, and Ethics 7. Research Methods 8. Security Operations 9. Technological Foundations for CS & Security Controls 10. Automation of Security Tasks and Data Analytics 11. CISO and Crisis Communication 12. Risk Management of Cyber-Physical Systems 13. Cybersecurity Auditing 14. Cybersecurity Economics & Supply Chain 15. Cybersecurity Education & Training Delivery I 16. Cybersecurity Education & Training Delivery II 17. Cybersecurity in Industry - Security of OT & CPS 18. Cybersecurity Law & Data Sovereignty 19. Machine and Deep Learning in Cybersecurity 20. Digital Forensics, Chain of Custody and eDiscovery 21. Threat Intelligence 	<p>–</p>
<p>Date of the contract: 06.08.2025</p> <p>Submission of the final version of the SAR: 06.10.2025</p> <p>Date of the onsite visit: 24.10.2025</p> <p>ONLINE audit</p>	
<p>Peer panel:</p> <p>Prof. Dr.-Ing. Sandro Leuchter, Technical University of Applied Sciences Mannheim;</p> <p>Prof. Dr. Thomas Meuser, University of Applied Sciences Niederrhein;</p> <p>Dr. Burkhard Petin, privacy/design GmbH;</p> <p>Nanshin Nansak, PhD candidate at Atlantic Technological University Sligo.</p>	

Representative of the ASIIN headquarter: Dr. Siegfried Hermes

Responsible decision-making committee: Certification Commission

Criteria used:

Standards for the Certification of (Further) Education and Training for courses and modules related to Computer Sciences, Technology, Natural Sciences and Business Economics as of 04.12.2022.

Standards and Guidelines for Quality Assurance in the European Higher Education Area as of 15 May 2015.

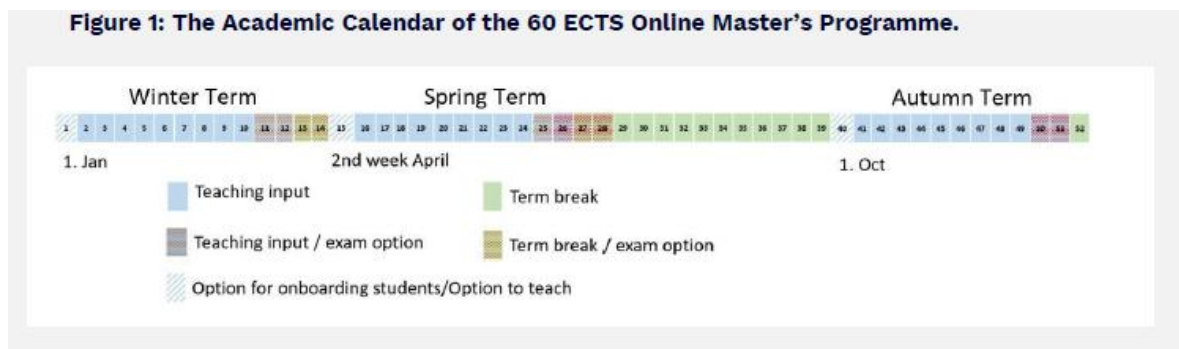
To facilitate the legibility of this document, only masculine noun forms will be used hereinafter. Any gender-specific terms used in this document apply to both women and men.

B Characteristics of the Modules

a) Name of the module	b) Degree awarded upon conclusion	c) Corresponding level of the European Qualifications Framework	d) Mode of Study	e) Duration & Credit Points	f) First time of offer & Intake rhythm	g) Number of students per intake	h) Fees
See list of 21 modules of the Online Joint Master's programme Cybersecurity Management and Data Sovereignty on p. 3 of this report	Certificate of completion	7	Part-time (roughly 10h per week)	12 weeks 5 CP	Thrice annually corresponding to Module offerings (Spring, Autumn and Winter) / Spring term 2026	5 – 50 (max. numbers to be set by lecturers; min. numbers set by Board of Directors)	350 EUR per module

For each **Module**, the intended module learning outcomes are defined in the respective module descriptions (Annex 7 to the SAR).

The modules can be studied within the following **timeline** (of the reference ONLINE Master's programme Cybersecurity Management and Data Sovereignty):



C Preliminary Note on the Procedure

The present certification procedure has been conducted in combination with an accreditation procedure for the Joint ONLINE Master’s Programme in Cybersecurity Management and Data Sovereignty, which has been developed within the framework of the Digital4Security project (Grant Agreement No. 101123430), co-funded by the European Union under the DIGITAL Europe Programme (DIGITAL-2022-SKILLS-03 – Advanced Digital Skills).

The modules are parts of the curriculum of the Joint Master’s programme. The experts’ judgment on many features of the Joint Master’s programme is therefore also relevant to the modules. Consequently, the certification report will refer to the accreditation report where applicable to avoid redundancy and to focus on those issues that have not yet been addressed in the accreditation process of the Joint Master’s programme. In this sense, the certification report reflects the fact that the accreditation of the Joint Master’s programme and the certification of the modules have been combined procedurally.

Therefore, the reader is explicitly referred to the accreditation report and related conclusions of the experts, where deficiencies and shortcomings of the Joint Master’s programme also pertain to the individual modules. This applies to both the preliminary and the final judgements of the experts.

The following table provides a synopsis of the reports and criteria addressed. It indicates where the experts’ judgement is already reflected in the accreditation report and where it is substantiated in the certification report.

Certification Standards	European Approach Acc. Standards	Subject
1.1	2	Learning outcomes (module level)
1.2	3	Contents, name and structure
1.3	5	Didactic and Teaching Methodology
1.4	4	Admission requirements
1.5	3	Workload
2	5	Examination System
3.1	6, 7	Staff and Student Support

C Preliminary Note on the Procedure

Certification Standards	European Approach Acc. Standards	Subject
3.2	7	Institutional Setting, Material and Financial Resources
4	9	Quality Management
5.1	8	Module Descriptions
5.2	8	Relevant Documents

Table 1: Synopsis of references to Accreditation Report for Joint Master's in Cybersecurity Management and Data Sovereignty

D Expert Report for the ASIIN Certificate

The following sections are based on the audit discussions the expert panel had with relevant stakeholder groups: Module coordinators, teaching staff, representatives from professional industry and business organisations, and students. In addition to the audit meetings, the expert panel relied on the documentation about the micro-credentials and the documentary respectively regulatory framework the universities provided before, during and after the audit.

1. Content, Structure and Implementation

Criterion 1.1 Learning outcomes of the course/module

Evidence:

- D4S Micro-credentials Self-Assessment Report (SAR)
- Module Handbook, Annex 7 to the SAR
- Student Handbook, Annex 8 to the SAR
- Cooperation Agreement, Annex 1 to the SAR
- Audit discussions

Preliminary assessment and analysis of the experts:

Cf. reference report Joint ONLINE Master's programme in Cybersecurity Management and Data Sovereignty, EA, Standards 2 and 3.

The expert panel confirms that the intended learning outcomes of the 21 modules submitted for certification are formulated clearly, are publicly available through the Module Handbook (Annex 7), and correspond to the knowledge, skills and competences expected at EQF Level 7. Each module defines concise outcome statements describing what learners will know, understand and be able to do upon completion, and these are explicitly linked to the overarching learning outcomes of the Online Master in Cybersecurity Management and Data Sovereignty. The mapping between module and programme outcomes convincingly demonstrates internal coherence and facilitates recognition of the micro-credentials within the joint degree.

The panel finds that the learning outcomes are *achievable and relevant*. Their scope reflects the interdisciplinary nature of cybersecurity – integrating managerial, legal, and technological dimensions – and they are oriented towards practical application in professional contexts. Discussions with lecturers and industry partners confirmed that the modules have been designed with explicit reference to the European Cybersecurity Skills Framework (ECSF) and to current labour-market needs. The participating institutions indicate their willingness to analyse trends in cybersecurity, risk governance and digital sovereignty through their Industry Advisory Board and the broader D4S network. These mechanisms will certainly help to ensure that the intended competences remain aligned with evolving sectoral requirements.

From a methodological standpoint, the modules' outcomes are *measurable and assessable* through defined learning activities and examination formats equivalent to those used in the accredited master's programme. Quality-assurance procedures foresee regular reviews of learning-outcome achievement by the Quality Service Committee and the Module Guarantors. Evidence from programme-level monitoring (surveys, workload analyses, achievement data) will also be used for the micro-credentials, ensuring consistent standards across both formats.

The panel particularly highlights the commitment of the consortium partners – UDS, MTU and UNIR, together with associated D4S partners – to establishing a coherent system of certified, stand-alone micro-credentials (see particularly, Cooperation Agreement (Annex 2), section 4.1, item E). This initiative demonstrates a strong strategic vision for flexible and stackable learning opportunities in cybersecurity education. The decision to exclude only the two Spanish modules (pending national regulation) and the Master's thesis from certification is reasonable and does not affect the integrity of the concept.

Preliminary assessment of experts:

Fully compliant <input checked="" type="checkbox"/>	Substantially compliant <input type="checkbox"/>	Partially compliant <input type="checkbox"/>	Non-compliant <input type="checkbox"/>
---	--	--	--

Criterion 1.2 Contents and Structure

Evidence:

- D4S Micro-credentials SAR
- Module Handbook, Annex 7 to the SAR
- Study and Exam Regulation, Annex 2 to the SAR
- Survey templates relating to the module level, Annex 5 to the SAR
- Internal Quality Handbook, Annex 4 to the SAR

- Audit discussions

Preliminary assessment and analysis of the experts:

Cf. reference report Joint ONLINE Master's programme in Cybersecurity Management and Data Sovereignty, EA, Standard 3.

The expert panel confirms that the content and structure of the 21 modules submitted for certification are coherently designed and enable learners to achieve the intended learning outcomes. The structure follows the pedagogical approach of the accredited joint master's programme, while ensuring each module's full autonomy as a stand-alone learning unit.

Each module is described in the Module Handbook (Annex 7) with clear specification of objectives, indicative content, workload distribution, teaching methods and assessment forms. The content demonstrates a deliberate balance between theoretical foundations and applied perspectives, covering managerial, technical, and regulatory dimensions of cybersecurity. Module topics – ranging from Incident Management and Threat Intelligence to Cybersecurity Economics, AI & Emerging Topics, and Cyber Law and Data Sovereignty – address the essential areas of the discipline reflecting current professional profiles derived from the European Cybersecurity Skills Framework (ECSF).

The Study and Examination Regulations (Annex 2) define the temporal and structural framework. According to this, each module runs over twelve weeks and is delivered entirely online via the D4S learning environment. The consistent 5-ECTS design of modules facilitates modular combination and potential stacking towards higher qualifications, including the Master's degree. The panel considers this standardisation an essential strength, supporting transparency, comparability and recognition across European higher-education systems.

The experts particularly note that all modules have been tested within the Digital4Security consortium and with industry partners prior to certification. Industry representatives confirmed that the content accurately mirrors current professional requirements and provides tangible added value for corporate training, continuing education and individual up-/re-skilling. The availability of modules as micro-credentials thus constitutes an effective mechanism for lifelong-learning participation and as an exit or entry point for professionals who may later continue into the full Master's programme.

The panel also observed that the consortium's system of Module Guarantors ensures clear academic responsibility for content and assessment, while allowing flexibility for teaching

contributions from other partner institutions. This governance model supports sustainability and continuous improvement of the modules.

Preliminary assessment of experts:

Fully compliant <input checked="" type="checkbox"/>	Substantially compliant <input type="checkbox"/>	Partially compliant <input type="checkbox"/>	Non-compliant <input type="checkbox"/>
---	--	--	--

Criterion 1.3 Didactics

Evidence:

- D4S Micro-credentials SAR
- Module Handbook, Annex 7 to the SAR
- Study and Exam Regulation, Annex 2 to the SAR
- Practical Guide for Lecturers, Annex 10 to the SAR
- Survey templates relating to the module level, Annex 5 to the SAR
- Internal Quality Handbook, Annex 4 to the SAR
- Audit discussions

Preliminary assessment and analysis of the experts:

Cf. reference report Joint ONLINE Master's programme in Cybersecurity Management and Data Sovereignty, EA, Standard 5.

The expert panel confirms that the didactic concept and methods applied in the 21 modules of the Cybersecurity Management and Data Sovereignty framework are appropriate for achieving the defined learning outcomes (cf. Standard 1.1) and are consistent with the content structures described under Standard 1.2. The didactic approach combines outcome orientation, learner engagement, and methodological consistency across all partners and delivery formats.

Each module employs a pedagogical design that explicitly links teaching and learning activities to the intended knowledge, skills and competences stated in the Module Handbook (Annex 7). The Practical Guide for Lecturers (Annex 10) and the Study and Examination Regulations (Annex 2) provide binding guidance on teaching methods, workload planning, and learner–teacher interaction. In the experts' view, this ensures that didactic choices are not arbitrary but systematically derived from learning-outcome formulations. The panel emphasises that the same quality requirements and pedagogical standards apply to the micro-credentials as to the Online Master's programme.

Didactic design is explicitly tailored to an online learning environment. The documentation and audit discussions show that lecturers shall make deliberate use of synchronous and asynchronous forms of instruction, structured feedback, and moderated peer exchange. It is noted that all teaching staff will be trained in digital pedagogy, and quality standards for online delivery – including accessibility, interaction frequency and clarity of instructional materials – are defined consortium-wide. The panel finds that these measures guarantee the effective implementation of e-learning concepts.

Furthermore, it is indicated that didactic effectiveness will be monitored through established quality-assurance instruments. Notably, student and instructor surveys (Annex 5) systematically gather evidence on teaching methods, clarity of materials and perceived contribution to outcome achievement. Results will be evaluated by the Quality Service Committee and reported to the Master’s Board for potential improvement actions. This periodical review will contribute to the continuous refinement of didactical methods based on empirical data.

Overall, the panel notes that that didactic methods encourage active student/learner participation, is appropriate to the target group of professionals and graduates, and demonstrably contributes to the achievement of the defined outcomes.

Preliminary assessment of experts:

Fully compliant <input checked="" type="checkbox"/>	Substantially compliant <input type="checkbox"/>	Partially compliant <input type="checkbox"/>	Non-compliant <input type="checkbox"/>
---	--	--	--

Criterion 1.4 Admission requirements

Evidence:

- D4S Micro-credentials SAR
- Module Handbook, Annex 7 to the SAR
- Study and Exam Regulation, Annex 2 to the SAR
- Survey templates relating to the module level, Annex 5 to the SAR
- Internal Quality Handbook, Annex 4 to the SAR
- Audit discussions

Preliminary assessment and analysis of the experts:

The expert panel confirms that admission requirements for the individual modules submitted for certification are defined transparently, are appropriate for the achievement of the

intended learning outcomes, and ensure that learners possess the necessary prior knowledge and competences for successful participation.

According to the Micro-credentials Self-Assessment Report and the Study and Examination Regulations (Annex 2), each module specifies entry conditions commensurate with its academic level and content focus. As most modules correspond to EQF Level 7, admission is normally open to applicants who hold a first-cycle qualification (Bachelor's degree or equivalent) or who can demonstrate comparable professional experience in a relevant field of digital technologies, management, or law. Modules that require specific prior competences (for example AI & Emerging Topics in Cybersecurity or Machine and Deep Learning in Cybersecurity) explicitly list them in the module descriptions contained in the Module Handbook. Conversely, modules of an introductory or cross-disciplinary nature (e.g. Cybersecurity Culture, Strategy & Leadership) can also be taken by qualified professionals from adjacent disciplines. The experts agree that this differentiation guarantees academic coherence while preserving accessibility for the intended target group of continuing-education learners.

The panel notes that, unlike admission to the Master of Science in Cybersecurity Management and Data Sovereignty – where cumulative ECTS volumes must satisfy Bologna-framework expectations – participation in a single certified module does not confer a degree and therefore does not require validation of total prior credit. For micro-credentials, the decisive criterion is the learner's ability to achieve the stated outcomes within the 5 ECTS scope. This rationale explains why, in contrast to the master's accreditation, no reservations arise regarding cumulative qualification volumes. The experts regard this distinction as consistent with the certification standards, which emphasise suitability rather than formal degree progression for stand-alone modules.

Admission procedures are implemented centrally through the D4S online platform, using harmonised forms and documentation across all consortium partners. Applicants are informed in advance about academic prerequisites, expected digital competences and technical requirements for online participation. The Practical Guide for Lecturers and the Welcome Module ensure that newly admitted participants receive orientation and support before commencing their studies. These mechanisms collectively satisfy the expectation that entry rules be transparent, fair, and supportive of learner success.

Quality assurance of admission procedures is embedded in the consortium's internal QA system. Accordingly, it can be expected that the Quality Service Committee periodically reviews admission data, learner profiles and subsequent achievement rates to verify that entry criteria continue to correspond to module difficulty and learning outcomes. The experts consider this feedback loop sufficient to maintain appropriateness over time.

Preliminary assessment of experts:

Fully compliant <input checked="" type="checkbox"/>	Substantially compliant <input type="checkbox"/>	Partially compliant <input type="checkbox"/>	Non-compliant <input type="checkbox"/>
---	--	--	--

Criterion 1.5 Workload

Evidence:

- D4S Micro-credentials SAR
- Module Handbook, Annex 7 to the SAR
- Study and Exam Regulation, Annex 2 to the SAR
- Survey templates relating to the module level, Annex 5 to the SAR
- Internal Quality Handbook, Annex 4 to the SAR
- Audit discussions

Preliminary assessment and analysis of the experts:

Cf. reference report Joint ONLINE Master's programme in Cybersecurity Management and Data Sovereignty, EA, Standard 3.

The expert panel confirms that the estimated workload for each module is realistic, transparent, and appropriate for achieving the intended learning outcomes within the designated timeframe. Each module corresponds to 5 ECTS credits, equivalent to approximately 125 hours of student work, and is structured for completion within a twelve-week teaching period, as defined in the Study and Examination Regulations and the Module Handbook.

The workload design mirrors that of the Online Master's programme in Cybersecurity Management and Data Sovereignty. During curriculum development, the consortium partners jointly determined the time allocations for learning activities and assessments, ensuring comparability across institutions and modules. The experts note that, while the workload calculation is identical for master's and micro-credential learners, the target groups may differ. Master's students typically pursue a structured full- or part-time study plan, whereas micro-credential learners are predominantly employed professionals engaging in short, focused learning units. Audit discussions and the SAR demonstrate that the consortium anticipated these differences and incorporated them into the instructional design. Modules are organised flexibly, combining asynchronous study phases with scheduled online interactions to allow working participants to distribute effort according to their availability. The experts regard this as an effective adaptation that preserves workload equivalence while accommodating the professional context of micro-credential learners.

In line with the Quality Assurance Handbook (Annex 4), the adequacy of workload estimates shall be monitored systematically. Accordingly, the Survey Templates (Annex 5) collect student feedback on perceived workload and its relationship to learning outcomes after each delivery cycle. Results shall be reviewed by the Quality Service Committee and, where necessary, lead to recalibration of module content or scheduling. The panel confirms that this procedure is appropriate to ensure continuous alignment between estimated and actual workload.

Final assessment of the experts after the comment of the Provider regarding criterion 1:

The partner HEIs did not comment on this criterion.

The panel considers the micro-credentials to be fully compliant with the standard. It reiterates its recommendation concerning the regular review of the modules (see below, chapter G, recommendation E 1).

Final assessment of experts:

Fully compliant <input checked="" type="checkbox"/>	Substantially compliant <input type="checkbox"/>	Partially compliant <input type="checkbox"/>	Non-compliant <input checked="" type="checkbox"/>
---	--	--	---

2. Examination: System, Policy and Implementation

Evidence:

- D4S Micro-credentials SAR
- Module Handbook, Annex 7 to the SAR
- Study and Exam Regulation, Annex 2 to the SAR
- Survey templates relating to the module level, Annex 5 to the SAR
- Internal Quality Handbook, Annex 4 to the SAR
- Audit discussions

Preliminary assessment and analysis of the experts:

Cf. reference report Joint ONLINE Master's programme in Cybersecurity Management and Data Sovereignty, EA, Standard 5.

The expert panel confirms that the system of examinations for the certified micro-credentials is conceptually coherent, outcome-oriented and implemented according to transparent and standardised procedures across all participating institutions. As the micro-credentials correspond directly to individual modules of the Online Master, the same regulatory

framework applies, as established in the Study and Examination Regulations (Annex 2). Assessment forms, grading criteria and procedural safeguards are therefore identical to those evaluated in the Master's accreditation.

Each module employs assessment methods clearly linked to its intended learning outcomes. Typical forms include proctored online examinations, case-study analyses, project reports and oral or multimedia presentations. The experts learned that assessment components are weighted to ensure that achievement of the defined knowledge, skills and competences (cf. Standard 1.1) can be demonstrated reliably and comparably among learners. The consistency of examination formats across modules supports transparency and recognition, particularly when micro-credentials are later stacked toward degree study.

The experts note that all examinations are organised digitally within the D4S learning environment. Technical and procedural instructions are or will be published in advance, guaranteeing equal treatment and accessibility. Procedures for make-up examinations, illness, and compensation for disadvantaged learners are clearly stated in the regulations and were verified during the audit. The consortium has also piloted secure online-proctoring solutions that fulfil data-protection requirements of all participating jurisdictions.

Quality assurance of examinations is embedded in the same internal monitoring system as for the Master's programme. The module guarantors are required to review examination results and to provide structured feedback to the Quality Service Committee, which reports to the Master's Board. Statistical analyses and learner surveys shall be used to check the appropriateness of examination demands and the relation between assessment and workload. The panel considers these procedures adequate and consistent with ESG 1.3 and 1.9.

Nevertheless, as already noted in the accreditation report, the governance structure could benefit from a higher degree of independence of the Examination Board from the Board of Directors (Master's Board). While the cooperation agreement clearly defines the existence of both bodies, some overlap in membership and decision-making authority remains, which could compromise procedural autonomy in the review or approval of examination results. The panel therefore recommends clarifying membership rules and reporting lines to guarantee institutional separation and independence.

In addition, the panel identified the need to refine the timeline of the appeals process, especially regarding the timeframe for a final decision. The current provisions specify the stages of appeal but do not define clear temporal limits for resolution, which may lead to uncertainty for learners. The consortium is advised to introduce explicit deadlines for each procedural step to enhance transparency and legal certainty.

Final assessment of the experts after the comment of the Provider regarding criterion 2:

The expert panel confirms its preliminary assessment and considers the standard concerning exams and the assessment system to be substantially fulfilled.

Independence of Examination Board:

Concerning independence of the Examinations Board, especially from the Board of Directors, the experts recognise the good intentions of the partner HEIs. Nevertheless, they repeat their caution as stated in the accreditation procedure of the Joint Online Master's programme in Cybersecurity Management and Data Sovereignty:

"The panel recognised the consortium's awareness of a potentially negative impact arising from the predominant decision-making powers of the Master's Board of Directors on the independence of the Examinations Board. The experts were convinced of the partner institutions' serious intention to reinforce the independent decision-making authority of the Examinations Board, not least through the appointment of "Board members who are distinct from the Programme Directors serving on the Master's Board" (Protocol of the Board of Directors, statement of the HEIs, p. 2).

However, the panel stressed that this personal separation is not required by the regulatory framework of the Cooperation Agreement. Moreover, the ambiguous wording in Section 4.2.4 of the Cooperation Agreement ("The Examinations Board is headed by the Master's Board of Directors.") continues to leave room for doubt regarding the Examinations Board's institutional status and independence. Due to this formal uncertainty, the panel concluded that a recommendation supporting the independence of the Examinations Board should be maintained (see below, section G, recommendation E 2)."

Timeline for appeals procedure

The experts positively note – as in the related paragraph of the Joint Online Master's programme – that this issue has been settled satisfactorily.

Final assessment of experts:

Fully compliant <input type="checkbox"/>	Substantially compliant <input checked="" type="checkbox"/>	Partially compliant <input type="checkbox"/>	Non-compliant <input type="checkbox"/>
--	---	--	--

3. Resources: Staff and Infrastructure

Criterion 3.1 Staff

Evidence:

- D4S Micro-credentials SAR
- Survey templates relating to the module level, Annex 5 to the SAR
- Internal Quality Handbook, Annex 4 to the SAR
- Teaching Staff CVs, Annex 9 to the SAR
- Practical Guide for Lecturers, Annex 10 to the SAR
- Audit discussions

Criterion 3.2 Institutional Environment, financial and material resources

Evidence:

- D4S Micro-credentials SAR
- Sample Supporting Partner Contract, Annex 14 to the SAR
- Sample Remuneration Manual, Annex 15 to the SAR
- Audit discussions

Preliminary assessment and analysis of the experts relating to standard 3:

Cf. reference report Joint ONLINE Master's programme in Cybersecurity Management and Data Sovereignty, EA, Standard 7.

3.1 Teaching Staff

The expert panel confirms that the composition and qualification of the teaching staff are, in principle, sufficient to guarantee achievement of the intended learning outcomes of the micro-credentials. Each module has a “Module Guarantor” responsible for academic content, assessment integrity and compliance with the quality standards of the Online Master in Cybersecurity Management and Data Sovereignty. This structure ensures that the same high-level expertise applied in the degree programme is also available to learners enrolling in individual modules as micro-credentials.

The documentation (Module Handbook, Annex 7; Staff CVs, Annex 9) demonstrates that lecturers possess appropriate scientific and professional qualifications at EQF Level 7 or above, complemented by certified competence in digital pedagogy. Many hold academic

or professional credentials in cybersecurity management, information law, and digital forensics. The audit confirmed that all faculty participate in the joint Train-the-Trainer scheme established under the D4S project, ensuring familiarity with consortium-wide didactic principles and assessment methods.

The experts note positively that the same academic staff teach both Master's and micro-credential cohorts, thereby ensuring consistency of standards, subject currency, and integration of industry perspectives. This arrangement also guarantees that quality assurance and workload monitoring (cf. Standards 1.3 and 1.5) extend equally to all delivery formats.

However, as identified in the accreditation of the Master's programme (see Accreditation Report, Standard 7), the governance structure for academic oversight remains incomplete. At the time of the audit, the Examination Board and the Quality Service Committee – both essential for quality assurance and staff coordination – had been designed as evidenced in the Cooperation Agreement but not yet formally appointed. The panel therefore considers it necessary to provide evidence of their establishment once it is available. Their full operation is necessary to confirm institutional capacity for sustainable delivery and staff management across partners.

3.2 Institutional Environment, Financial and Material Resources

The experts find that the institutional environment of the consortium provides a sound and sustainable foundation for the implementation of the micro-credentials. The participating universities are all established higher-education institutions with proven capacity for online provision and adequate human, financial and technological resources. The D4S infrastructure, including the central Moodle-based learning platform and the Full Fabric learner-management system, is fully operational and accessible to all partners. Financial sustainability beyond the EU funding phase has been addressed by the institutions' commitment to integrate the modules into their continuing-education portfolios.

Regarding learning resources, the consortium ensures that participants in micro-credentials have access to the same digital tools, tutorials and support services as Master's students, including the Welcome Module and online tutoring. The panel verified that students benefit from electronic library services of their enrolling institution. Nevertheless, in line with the expectation formulated in the Master's accreditation, the experts request explicit confirmation that this access includes at least two major subject-related scientific collections – namely the ACM Digital Library, IEEE Xplore, or Springer Nature Link – or, alternatively, a clear statement on the actual scope of available resources. Access to these databases is considered essential to guarantee the academic depth appropriate for EQF Level 7 modules in cybersecurity management and data sovereignty.

Final assessment of the experts after the comment of the Provider regarding criterion 3:

The expert panel considers the partner HEIs substantially compliant with the requirements of the criterion.

Establishment of the governing bodies

From the protocol of the first meeting of the Board of Directors (§ 2), the experts learned that the members for the governing bodies of the joint Master's programme had been appointed and the corresponding bodies (Examinations Board, Joint Admissions Board, and Quality Service Committee) established accordingly. As a result, the originally conceived requirement to this end has been waived.

Access to digital library resources

In its response to the report, the HEI consortium explicitly approved the acquisition of licences for two major subject-related scientific collections, prioritised as follows: (1) ACM Digital Library, (2) IEEE Xplore, and (3) Springer Nature Link. According to the statement, the D4S platform management team is authorised to procure these resources up to a specified annual cost-ceiling. The expert team considered this re-affirmation to be sufficiently mitigating concerns in this regard and concluded to cancel a related requirement.

Final assessment of experts:

Fully compliant <input type="checkbox"/>	Substantially compliant <input checked="" type="checkbox"/>	Partially compliant <input type="checkbox"/>	Non-compliant <input type="checkbox"/>
--	---	--	--

4. Quality Management: Monitoring and Continuous Improvement

Quality assurance and enhancement
--

Evidence:

- D4S Micro-credentials SAR
- Survey templates relating to the module level, Annex 5 to the SAR
- Internal Quality Handbook, Annex 4 to the SAR
- Audit discussions

Preliminary assessment and analysis of the experts:

Cf. reference report Joint ONLINE Master's programme in Cybersecurity Management and Data Sovereignty, EA, Standard 9.

The expert panel confirms that the consortium operates a coherent and comprehensive quality-management covering all activities relevant to the planning, implementation and evaluation of the micro-credentials. The approach builds directly upon the quality framework established for the Online Master (see Accreditation Report, Standard 9 – Quality Assurance), ensuring identical procedures and data flows at the module level.

Responsibility for QA is anchored in a clearly defined governance structure. The Quality Service Committee – comprising representatives of all three awarding institutions and chaired by the programme coordinator at UDS – is charged with monitoring teaching quality, assessment practices, learner satisfaction and workload alignment. Each module's Guarantor must submit a standardised module review after completion, containing key indicators on achievement rates, workload, and examination performance. These reports, together with aggregated survey results (see Annex 5 – Survey Templates), are to be analysed by the Committee and presented to the Master's Board for strategic decisions. The panel found this process to be functional, systematic, and appropriate for continuous improvement.

The experts noted a high level of quality culture among staff and management across all partner institutions. During the audit, module coordinators demonstrated detailed knowledge of the QA instruments and their use for evidence-based enhancement. The consortium's digital environment facilitates data collection and transparency. While the Full Fabric management system automatically records enrolment, assessment and satisfaction data, the D4S platform supports structured feedback from both students and instructors. The resulting data sets enable longitudinal analyses of learner performance and module effectiveness. The panel also learned that external stakeholders – particularly representatives from the Industry Advisory Board – already were and will be regularly involved in reviewing the relevance and up-to-dateness of module content (see also Standards 1.1 and 1.2). This integration of professional feedback will ensure that the quality-assurance cycle includes labour-market perspectives, aligning academic development with evolving industry needs. The experts consider this mechanism exemplary for a continuing-education context.

Finally, the QA procedures cover both formative and summative aspects. They address not only compliance and documentation but also pedagogical reflection and staff development. It can be expected that results are shared within the consortium, and identified good

practices are disseminated through joint staff-training sessions. The panel considers this systematic feedback loop a key strength of the D4S model.

Final assessment of the experts after the comment of the Provider regarding criterion 5:

The partner HEIs did not comment on the criterion.

The expert panel considers the requirements for quality assurance to be fully met. Accordingly, the micro-credentials fully comply with the standard.

Final assessment of experts:

Fully compliant <input checked="" type="checkbox"/>	Substantially compliant <input type="checkbox"/>	Partially compliant <input type="checkbox"/>	Non-compliant <input type="checkbox"/>
---	--	--	--

5. Documentation and Transparency

Criterion 5.1 Module descriptions

Evidence:

- D4S Micro-credentials SAR
- Module Handbook, Annex 7 to the SAR
- Audit discussions

Criterion 5.2 Relevant documents

Evidence:

- D4S Micro-credentials SAR
- Module Handbook, Annex 7 to the SAR
- Student Handbook, Annex 8 to the SAR
- Study and Exam Regulation, Annex 2 to the SAR
- Survey templates relating to the module level, Annex 5 to the SAR
- Sample Student Agreement, Annex 13 to the SAR
- Sample Supporting Partner Agreement, Annex 14 to the SAR
- Internal Quality Handbook, Annex 4 to the SAR
- Audit discussions

Preliminary assessment and analysis of the experts relating to Standard 5:

Cf. reference report Joint ONLINE Master's programme in Cybersecurity Management and Data Sovereignty, EA, Standard 9.

5.1 Module Descriptions

The expert panel recognises that the consortium has developed a consistent documentation framework for all modules to be certified as micro-credentials. The Module Handbook follows a standardised template that specifies learning outcomes, indicative content, assessment types, workload, and intended competences. The descriptions reflect the same structure and academic logic as those used for the accredited Online Master (see Accreditation Report, Standard 8 – Transparency and Documentation).

Nevertheless, during the audit the panel identified deficiencies in completeness and accessibility of the module documentation. While the overall format is clear and aligned with EQF Level 7 expectations, most module descriptions lacked information on the frequency of delivery and the responsible module coordinator or lecturer. These omissions limit transparency for prospective learners and teaching staff and must be corrected before certification.¹ In addition, the panel recommends that a revision history be added to each module description, documenting the date and scope of any updates. This measure would strengthen version control and contribute to the overall quality and traceability of curriculum development.

Furthermore, although the SAR indicates that the module descriptions will be published on the consortium's digital learning platform after accreditation, at the time of review they were not yet accessible to the relevant stakeholders. The panel therefore sees the necessity to make the revised module information publicly available – at least through the D4S portal and institutional websites – to ensure that learners and instructors have consistent reference points for planning, enrolment, and delivery.

5.2 Relevant Documents

The panel confirms that the consortium has prepared all major documents governing the establishment and implementation of the certified modules – such as the Study and Examination Regulations, the Quality Handbook, and the Cooperation Agreement. These documents collectively define the roles and responsibilities of stakeholders, the delivery and assessment of modules, and the issuance of certificates. In this context, the experts also

¹ Cf. ECTS User's Guide with further information, pp. 45-57, 57, available on the internet: https://education.ec.europa.eu/sites/default/files/document-library-docs/ects-users-guide_en.pdf (Access: 2025-11-08).

note that UDS on behalf of the consortium will be the only certificate-issuing institution for all micro-credentials delivered in the framework of the ONLINE Master's programme.

In accordance with certification standards, the mentioned provisions must be in existence and operational, even if not all of them will be publicly available. However, at the time of the audit, the consortium had not yet provided evidence of publication for the major study-related documents – specifically the Study and Examination Regulations, the Module Handbook, the Student Handbook, the Quality Handbook, and procedures for complaints and appeals. The expert panel therefore considers it indispensable that these key materials are implemented and accessible to the relevant stakeholder groups, including learners, teaching staff, and external groups. Publication may occur through the consortium's central website or other appropriate digital means.

Subject to fulfilment of these conditions, the panel considers the documentation system generally well structured and comprehensive. Once updated and made accessible, it will ensure transparency of responsibilities, regulations, and learning outcomes in line with certification expectations.

Final assessment of the experts after the comment of the Provider regarding criterion 5:

The panel considers the partner HEIs to be substantially compliant with the criterion on transparency and documentation.

Module Handbook

Module contact persons: The experts acknowledge that the contact persons for each module were listed in the "Contacts" chapter (pp. 137–138) of the submitted PDF documents, as pointed out by the partner HEIs. However, this does not apply to the published version on the D4S website, for example, where this chapter has been omitted in line with the strict requirement of the submitted versions. It is difficult to understand why the names of the contact persons should be omitted from the published versions of the Module Handbook. This is especially confusing given that they are provided elsewhere on the programme website, as apparently planned and demonstrated by the partner HEIs. The panel therefore still recommends including the names of the responsible module coordinators/lecturers in the module descriptions.

Module delivery: In general, it is highly advisable to include as much information as possible in a central information source, such as the Module Handbook. However, regarding the frequency of module delivery, the experts recognise that this may vary according to enrolment scenarios. Therefore, they accept the specifications provided in a separate document ("Course Scheduling Manual") until the referential online Master's programme is fully operational, considering this sufficient.

Version history: The panel acknowledges that the governance section of the study-related documents already includes a version history. No further action is needed in this regard.

Accessibility of key documents: As with the documentary relating to the referential Joint Online Master's programme, the panel acknowledges the legal barriers currently preventing the full publication of the relevant study documents. At the same time, the experts noted the provisional publication of the key documents on a D4S website. They are confident that publication of the module-related orders, manuals and guidelines will follow as soon as the legal situation in Ireland permits. The panel does not consider it necessary to request further evidence.

Final assessment of experts:

Fully compliant <input type="checkbox"/>	Substantially compliant <input checked="" type="checkbox"/>	Partially compliant <input type="checkbox"/>	Non-compliant <input type="checkbox"/>
--	---	--	--

E Additional Documents

No additional documents needed.

F Comment of the Provider (24.11.2025)

The institution provided a detailed statement, referred to in the final assessment of the expert panel at the end of each criterion. Furthermore, one additional document was provided:

- D4S Online Master's Course Scheduling Manual.

G Summary: Peer recommendations (04.12.2025)

Considering the additional information and the comments given by the partner HEIs, the experts summarize their analysis and **final assessment** for the award of the ASIIN certificate as follows:

Modules	ASIIN Certificate	Maximum duration of certification	Alignment to a Qualification Framework Level
21 Modules (from the joint Online Master's programme Cybersecurity Management and Data Sovereignty according to the list below)	awarded without requirements	30.09.2031	7

No.	Module	ECTS	Delivering Partners ¹
1	Communication Design for Cybersecurity	5	UDS
2	Business Resilience, Incident Management & Threat Response	5	MTU
3	AI & Emerging Topics in Cybersecurity	5	UDS
4	Cybersecurity Culture, Strategy & Leadership	5	VMU/ATAYA
5	Enterprise Architecture, Infrastructure Design and Cloud Computing	5	UPB
6	Law, Compliance, Governance, Policy, and Ethics	5	UNIBS
7	Research Methods	5	UNI KO
8	Security Operations	5	CY CERGY
9	Technological Foundations for CS & Security Controls	5	UPB
10	Automation of Security Tasks and Data Analytics	5	UNIRI
11	CISO and Crisis Communication	5	VMU/ATAYA
12	Risk Management of Cyber-Physical Systems	5	POLIMI/CEFRIEL
13	Cybersecurity Auditing	5	VMU/ATAYA
14	Cybersecurity Economics & Supply Chain	5	MRU
15	Cybersecurity Education & Training Delivery I	5	BUT
16	Cybersecurity Education & Training Delivery II	5	UPB
17	Cybersecurity in Industry - Security of OT & CPS	5	POLIMI
18	Cybersecurity Law & Data Sovereignty	5	BUT
19	Machine and Deep Learning in Cybersecurity	5	UNIRI
20	Digital Forensics, Chain of Custody and eDiscovery	5	UPB
21	Threat Intelligence	5	UPB

Recommendations

For all modules

- E 1. (ASIIN 1.2) It is recommended to regularly review the individual modules to keep them aligned to scientific developments and market demands.
- E 2. (ASIIN 2) It is recommended that the independence of the examination board against the Board of Directors be strengthened.
- E 3. (ASIIN 5.1) It is recommended to include information about the contact persons/lecturers in the module descriptions.

H Decision of the Certification Commission (16.12.2025)

Assessment and analysis for the award of the ASIIN Certificate:

The Certification Commission discusses the procedure and follows the assessment and judgement of the expert team without any changes.

The Certification Commission decides to award the following seals:

Modules	ASIIN Certificate	Maximum duration of certification	Alignment to a Qualification Framework Level
21 Modules 1. Communication Design for Cybersecurity 2. Business Resilience, Incident Management & Threat Response 3. AI & Emerging Topics in Cybersecurity 4. Cybersecurity Culture, Strategy & Leadership 5. Enterprise Architecture, Infrastructure Design and Cloud Computing 6. Law, Compliance, Governance, Policy, and Ethics 7. Research Methods 8. Security Operations 9. Technological Foundations for CS & Security Controls 10. Automation of Security Tasks and Data Analytics 11. CISO and Crisis Communication 12. Risk Management of Cyber-Physical Systems 13. Cybersecurity Auditing 14. Cybersecurity Economics & Supply Chain 15. Cybersecurity Education & Training Delivery I 16. Cybersecurity Education & Training Delivery II 17. Cybersecurity in Industry - Security of OT & CPS 18. Cybersecurity Law & Data Sovereignty 19. Machine and Deep Learning in Cybersecurity 20. Digital Forensics, Chain of Custody and eDiscovery 21. Threat Intelligence	awarded without requirements	30.09.2031	7

Recommendations

For all modules

- E 1. (ASIIN 1.2) It is recommended to regularly review the individual modules to keep them aligned to scientific developments and market demands.
- E 2. (ASIIN 2) It is recommended that the independence of the examination board against the Board of Directors be strengthened.
- E 3. (ASIIN 5.1) It is recommended to include information about the contact persons/lecturers in the module descriptions.