Digital4Security
Shaping Europe's cyber future

D3.3. EU-Recognized Certification and Accreditation: Demonstrator, Pilot, Prototype.

Project: 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03

Table of Contents

1. THE DIGITAL4SECURITY CONSORTIUM

The Digital4Security Consortium is a dynamic pan-European partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management programme, developed and delivered by the best cybersecurity talent from Europe and worldwide. Table 1 lists the Higher Education Institutions (HEIs) jointly offering the master's degree, while Table 2 presents additional consortium partners, including industry stakeholders.

Table 1: Academic Partners (Higher Education Institutes) Offering the Joint Degree Program

No.	Partner	Abbreviation	Country
1	Universitatea Nationala de Stiinta si Technologies Politehnica Bucuresti	POLITEHNICA B.	Romania
2	National College of Ireland	NCI	Ireland
3	German University of Digital Science	UDS	Germany
4	University of Rijeka	UNIRI	Croatia
5	Università degli Studi di Brescia	UNIBS	Italy
6	Politecnico di Milano	POLIMI	Italy
7	Universität Koblenz	UNI KO	Germany
8	CY Cergy Paris Université	CY	France
9	Mykolo Romerio Universitetas	MRU	Lithuania
10	Universidad Internacional de La Rioja	UNIR	Spain
11	Brno University of Technology	BRNO UNIVERSITY	Czech Republic
12	Munster Technological University	MTU	Ireland
13	Vytautas Magnus University	VMU	Lithuania

Table 2: Associate Partners

No.	Associated Partner	Abbreviation	Country
14	DIGITAL TECHNOLOGY SKILLS LIMITED	DTSL	Ireland
15	IT@CORK ASSOCIATION LIMITED LBG	IT@CORK	Ireland

16	SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	SKILLNET	Ireland
17	ADECCO FORMAZIONE SRL	ADECCO TRAINING	Italy
18	ADECCO ITALIA HOLDING DI PARTECIPAZIONE E SERVIZI SPA	ADECCO GROUP	Italy
19	ADECCO ITALIA SPA	Adecco Italia	Italy
20	CEFRIEL SOCIETA CONSORTILE A RESPONSABILITA LIMITATA SOCIETA BENEFIT	CEFRIEL	Italy
21	ATAYA & PARTNERS	Ataya	Belgium
22	CYBER RANGES LTD	Cyber Ranges	Cyprus
23	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	FHG	Germany
24	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	NASK	Poland
25	POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	CMIP	Poland
26	SCHUMAN ASSOCIATES SCRL	SA	Belgium
27	CONTRADER SRL	Contrader	Italy
28	INDEPENDENT PICTURES LIMITED	indiepics	Ireland
29	MATRIX INTERNET APPLICATIONS LIMITED	MATRIX	Ireland
30	PROFIL KLETT D.O.O.	PROFIL KLETT	Croatia
31	SERVICENOW IRELAND LIMITED	ServiceNow	Ireland
32	EUROPEAN DIGITAL SME ALLIANCE	DIGITAL SME	Belgium
33	DIGITALEUROPE AISBL*	DIGITALEUROPE	Belgium
34	TERAWE TECHNOLOGIES LIMITED	TERAWE	Ireland
35	BANCO SANTANDER SA	BANCO SANTANDER /Santander	Spain
36	RED OPEN S.R.L.	RED OPEN S.R.L.	Italy
37	PEARSON BENELUX	PEARSON B.	Netherlands

The HEIs, in conjunction with the Digital4Security consortium's industry partners, have collaborated and cooperated to jointly develop and design the master's programme and its curriculum.

2. Document Control Information

Project	Digital4Security
Document Title	D3.3. EU-Recognized Certification and Accreditation: Demonstrator, Pilot, Prototype.
Work Package Number	WP3
Deliverable Number	D3.3
Lead Beneficiary	German University of Digital Science (UDS)
Project Coordinator:	National University of Science and Technology Politehnica of Bucharest (NUSTPB)
Dissemination Level	PU - Public
Authors	Julia von Thienen (main author), together with all academic partners co-developing the accreditation documents (Annex I, and excerpts in the main text)
Reviewers	Lucia Grilli, Florin Pop, T3.3 Co-Lead and task members
Description	EU Recognised Certification & Accreditation
Status	Submitted
Delivery Date	31.12.2024
Due date	31.12.2024
Approval Date:	Pending

Revision history

Version	Date	Modified by	Comments
1	5.12.2024	Julia von Thienen	An initial draft was circulated to over 50 project members, with a focus on T3.3 and WP1, for review.
2	18.12.2024	Julia von Thienen	Following coordinated feedback via email and T3.3 weekly calls, a revised version was uploaded to Teams for further input.
3	20.12.2024	Julia von Thienen	Final documents were prepared based on additional input from Quality Assurance (Lucia Grilli) and the D4S Task Force.
4	31.12.2024	Florin Pop	A comprehensive PDF was compiled from the reviewed document sources.
5	11.04.2025	Julia von Thienen	Addition of Document Control Information.

3. OBJECTIVES OF DELIVERABLE D3.3

Deliverable D3.3 is a **"**DEM — Demonstrator, pilot, prototype**"** that emerges from task T3.3, dedicated to the following objectives:

> "The setup of a D4S Certification **Model** building on the **certification standards catalogue** the consortium will adopt.
> **The processes help to check and secure the quality of the modules and sub-programs in order to guarantee the quality of the online program**. Directly based on that flexible test centres for remote and in-person examinations will be implemented."
> (D4S Grant Agreement, p. 83, emphasis added)

This deliverable ties in closely with two other tasks.

Task T2.3 is defined as a parallel task to T3.3 in the timeline of the Grant Agreement, also focusing on industry certification and accreditation, with an emphasis on designing pathways and timelines:

> "Define Certification, Accreditation and Evaluation **Pathways** that will provide EU recognised qualifications.
> Certification partners will set up test centres in each Higher Education Institution and / or online. [...] **Set up a timeline with partners for university accreditations."**
> (D4S Grant Agreement, p. 81, emphasis added)

The task detailing the accreditation process most extensively is T6.1, running from M1-M48.

> "The Academic Accreditation process will be **achieved in phases**, first in Germany, then at EU level, then as a Virtual University [...]. As part of the sustainability strategy we will build sustainability into the Masters programmes by **defining standards and criteria** for the programme that **ensures close connection of the curricula and learning programme specification with recognized European instruments**, standards and tools [...]. The programme curriculum and **content will be refreshed** after each 2 or 3 year Masters. **Students will be surveyed** after the first year to collect their feedback which will be brought back to the Industry Advisory Board for discussion and recommendations on content updates. We will also undertake **surveys of SMEs and companies** each year of the project as part of the Quality Assurance Plan."
> (D4S Grant Agreement, p. 89, emphasis added)

As these three tasks schedule highly overlapping activities and outcomes, deliverable D3.3 presents progress across all three tasks, focusing on prototypes that integrate quality assurance mechanisms, certification pathways, and accreditation models.

Subsequently, we will first discuss the function and standards of prototypes, tracing what this means for academic accreditation, industry certification and quality assurance, subsequently presenting the outcomes and drawing conclusions.

4. Prototyping and Quality Standards for Certification and Accreditation Models

Deliverable D3.3 is defined as a prototype, thus requiring clarification of what this means in the context of industry certification and academic accreditation.

Prototyping is a well-established and extensively researched approach in engineering and design. Leveraging this methodology in a well-informed manner helps optimize the design and implementation of a master's program in Cybersecurity Management & Data Sovereignty. Prototypes serve as representations of the envisioned final products or services, with a primary function being to fast-track project progress and improve final design outcomes.

Dow et al. (2009) describe a canonical prototyping iteration as encompassing four key steps: envisioning possibilities, creating a prototype to embody one possibility, gathering feedback on the prototype, and re-evaluating constraints.

Parallel Prototyping: Enhancing Design Quality

Research highlights the effectiveness of parallel prototyping, which involves exploring multiple models or options simultaneously. For instance, in a study by Dow et al. (2010), participants designed advertisements for the same client. While all participants created five prototypes and received feedback before finalizing their designs, the experimental group followed a parallel prototyping approach, designing three models simultaneously and refining two based on feedback before delivering their final product. By contrast, the control group adopted a serial approach, refining one design iteratively. The parallel approach significantly outperformed the serial method in terms of ad effectiveness, measured by click rates. This underscores the importance of comprehensively exploring design spaces by evaluating multiple options to identify the best approach.

Practice Testing: Accelerating Learning and Improving Outcomes

Despite hesitations to test prototypes prematurely, research demonstrates the benefits of practice tests even when designs are incomplete. In an experiment by Dow et al. (2011), participants designed vessels to protect raw eggs dropped from increasing heights, with all groups allotted the same 25 minutes. The experimental group conducted practice tests during the design phase, while the control group planned and built without intermediate testing. Despite initial discomfort with testing incomplete designs, the experimental group achieved solutions that performed nearly twice as well as the control group's. This highlights the value of practical testing to accelerate learning and achieve higher-quality outcomes within the same timeframe.

Implications for Industry Certification and Academic Accreditation

Based on these insights, we endorse the following quality criteria for demonstrators, pilots, and prototypes in the context of industry certification and academic accreditation:

- **Exploration of Multiple Models**: Each domain should consider multiple options to ensure a comprehensive exploration of possibilities and identification of optimal solutions. This aligns with the review of different possible certification models (Section 4) and accreditation models (Section 6).
- **Fast-Tracked Implementation and Testing**: Once optimal models are identified, emphasis should shift to rapid implementation and testing to accelerate learning and project progress. For industry certification, this can unfold fully once the master's program is launched, with progress reviewed in Section 5. For accreditation, a detailed implementation process has already been implemented (Section 7).

Building on these foundations, the report further highlights the development of:

- **Governance Bodies**: Structures for the Joint Programme in Cybersecurity Management and Data Sovereignty (Section 8).
- **Quality Assurance Mechanisms**: Internal tools and processes aligned with European standards and accreditation requirements (Section 9).
- **Key Insights**: Comprehensive findings on accreditation and joint degree offerings in Europe, prepared for presentation to EU bodies (Section 10).

5. Different Certification Models

For a cybersecurity master's program, certification options should align with technical competencies and industry standards. Certifications like CISSP (Certified Information Systems Security Professional) or CISM (Certified Information Security Manager) focus on managerial and governance skills, complementing advanced coursework. Technical certifications such as CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), or vendor-specific certifications from AWS or Microsoft Azure validate practical expertise in areas like ethical hacking or cloud security.

While these certification options address diverse learning and performance domains through testing, more fundamental questions about certification models must be addressed. Key considerations include the responsibility for overseeing certification processes, and the format of testing - whether it will be conducted onsite, online, or offered in a hybrid format. Following consultations within the consortium, the following certification models were identified, each highlighting unique advantages, challenges, and varying levels of suitability.

HEI-Led Certification

How It Works: Universities organize and manage the certification process, either by designing their own tests or integrating recognized frameworks. The format can be online, onsite, or hybrid, leveraging existing institutional resources.
Estimated Cost: up to 20,000 € per institution for setup and maintenance, depending on how much testing infrastructure is already available.
Advantages:

- High institutional control ensures alignment with academic standards.
- Leverages university resources (e.g., labs, proctors, digital platforms).
- Strengthens the university's brand and credibility.

Disadvantages:

- Resource-intensive setup and maintenance.
- May lack industry recognition compared to established certifications.

Fastest and Most Reliable? Moderate; consistency is ensured, but institutional processes may introduce delays.

Industry Partner-Led Certification

How It Works: Industry partners oversee the certification process, offering either proprietary or vendor-neutral exams. They ensure alignment with industry needs and leverage existing certification frameworks.
Estimated Cost: €200–500 per student for certification exams.
Advantages:

- High industry alignment enhances employability.
- Established platforms ensure smooth and efficient processes.
- Reduces the administrative burden on universities.

Disadvantages:

- Less academic control over the certification's content and format.
- Potential misalignment with educational goals or curriculum.
- Costs may deter some students.

Fastest and Most Reliable? High; industry platforms are efficient and widely trusted.

Third-Party Certification Providers

How It Works: Independent providers administer exams, typically offering globally recognized certifications (e.g., AWS, Microsoft, CISSP). These entities manage the entire process, from exam design to delivery.
Estimated Cost: €300–600 per student for certification exams.
Advantages:

- Globally recognized certifications enhance credibility and transferability.
- Minimal infrastructure required from universities or industry partners.
- Proven expertise in testing and certification.

Disadvantages:
- High per-student costs.
- Limited customization or integration with academic programs.

Fastest and Most Reliable? High; third-party systems are efficient and scalable.

EU-Centralized Certification

How It Works: A centralized EU body coordinates and manages the certification process, ensuring harmonized standards and recognition across member states. Examples include issuing certificates such as *EU Cybersecurity Specialist* or *European Data Sovereignty Professional*, which align with EU frameworks like ENISA guidelines.
Estimated Cost: €50,000–100,000 for setup and coordination, plus €10–20 per test.
Advantages:
- EU-wide recognition ensures high credibility and transferability.
- Standardization simplifies implementation across institutions.
- Supports international collaboration and mobility.

Disadvantages:
- Requires significant coordination and negotiation among stakeholders.
- EU-level processes can delay implementation.
- High initial costs for setup and ongoing coordination.

Fastest and Most Reliable? EU processes are often time-consuming, but reliable once established.

An overview of these options is provided in Table 3.

Table 3: Different Models of Certification Implementation by Varying Responsible Bodies

Model	Estimated Cost	Advantages	Disadvantages	Fastest and Most Reliable?
HEI-Led Certification	up to €20,000 for setup	High control, academic alignment, institutional branding	Resource-intensive, lower industry recognition	Moderate
Industry Partner-Led	€200–500 per exam	Strong industry alignment, efficient processes	Less academic control, potential cost barrier	High
Third-Party Providers	€300–600 per exam	Globally recognized, minimal infrastructure required	High cost per student, limited customization	High
EU-Centralized	€50,000–100,000 setup	EU-wide recognition, standardized processes	Slow implementation, high initial cost	Low

Likewise, different options exist for online, onsite or hybrid certification models.

Online-Only Certification

How It Works: Exams are conducted entirely online, typically by using secure proctoring platforms to prevent cheating. This approach eliminates the need for physical infrastructure.
Estimated Cost: €5–50 per test including proctoring, plus potential setup costs for custom platforms (€5,000–50,000)
Advantages:

- Highly scalable and accessible for students worldwide.
- Reduces logistical challenges (e.g., no need for physical facilities or student mobility).
- Can incorporate adaptive testing technology for personalized experiences.

Disadvantages:

- Requires robust IT infrastructure and reliable internet access for all participants.
- Cybersecurity concerns, including risks of cheating and data breaches.
- Limited by the technical capacity of proctoring software to handle all test types (e.g., highly interactive tasks).

Fastest and Most Reliable? High; well-established platforms ensure rapid deployment and smooth execution.

Onsite-Only Certification

How It Works: Exams are conducted in physical locations, such as university facilities, industry testing centers, or dedicated certification hubs. Proctors oversee testing to ensure security and fairness.
Estimated Cost: €10–60 per test, plus potential setup costs (€30,000-100,000, depending on scale).
Advantages:

- Provides controlled and secure testing environments, reducing cheating risks.
- Allows for in-person support and accommodations, benefiting students with accessibility needs.
- Builds trust in certification processes, particularly for high-stakes exams.

Disadvantages:

- Limited flexibility, especially for remote or international students.
- Logistically intensive, requiring coordination of facilities, proctors, and schedules.
- Higher environmental impact due to travel and physical infrastructure.

Fastest and Most Reliable? Moderate; logistics can slow implementation, but in-person oversight ensures reliability.

Hybrid Certification

How It Works: Students can choose between taking certification exams online or onsite. Institutions or industry partners provide both modes, ensuring flexibility and accessibility.
Estimated Cost: €15,000–70,000 for dual infrastructure setup, plus €5–60 per test.
Advantages:

- Balances flexibility for remote learners with reliability of onsite proctoring.
- Ideal for diverse student populations with varying access to technology or testing centers, and different preferences.
- Can be scaled to suit different needs (e.g., technical versus managerial certifications).

Disadvantages:

- Higher initial setup costs due to dual infrastructure.
- Increased complexity in managing two modes of testing.

Fastest and Most Reliable? High for online; moderate for onsite due to logistical considerations.

An overview of these options is provided in Table 4.

Table 4: Different Models of Certification Locations

Option	Estimated Cost	Timeline	Advantages	Disadvantages
Online-Only	€5–50 per test €5,000–50,000 setup	6–12 months	Scalable, accessible, low logistical burden	Cybersecurity risks, requires robust IT infrastructure
Onsite-Only	€10–60 per test €30,000-100,000 setup	9–18 months	Secure environment, trusted processes, in-person help	Logistically complex, limited flexibility
Hybrid	€5–60 per test €15,000–70,000 setup	12–18 months	Combines flexibility with reliability; accessible	High complexity, costly dual infrastructure

6. Selected Pathways and Industry Certification Model

To provide the best services to students and in alignment with the Grant Agreement, the consortium has opted for a hybrid certification model. Furthermore, certification will be offered by industry partners within the consortium, with the option to collaborate with third-party providers to expand the range of certification opportunities. While 2–3 certification exams shall be included in the student fees, students will be responsible for covering the costs of any additional certification tests. Academic training within the master's program will prepare students for these exams, as outlined below.

The planned industry certification in the Digital4Security project is contingent upon students being actively enrolled in the master's program. The dual approach of allowing them to earn both an academic degree and industry certifications in parallel optimizes their job readiness for the cybersecurity market. For successful implementation, the master's program must first be launched to enable for the testing of specific certification pathways. At present, the consortium is focused on finalizing the curriculum and preparing pilot course tests, while also refining the details of the chosen certification model.

To ensure flexibility in terms of educational pathways, meeting diverse learners and industry needs, the curriculum of the Master's Degree Programme in Cybersecurity Management and Data Sovereignty has been designed in such a way as to equip students with the necessary skills for various ENISA profiles. ENISA (the European Union Agency for Cybersecurity) outlines specific competencies and skills relevant to different job roles in the cybersecurity field.

Based on the market analysis conducted in collaboration with industry partners, several job profiles have been identified, and corresponding curricula have been developed to ensure professional preparation. A survey among all HEIs confirmed the inclusion of eight profiles in the Master's programme, though a reduction to six of them is still being considered to prioritize managerial skills. The various pathways prepared allow students to specialize in areas such as:

1. **Chief Information Security Officer (CISO)** - Focused on strategic leadership and management of an organization's cybersecurity approach (Fig. 1).
2. **Cyber Legal, Policy, and Compliance Officer** - Concentrating on the legal and regulatory aspects of cybersecurity, ensuring compliance with relevant laws and policies (Fig. 2).
3. **Cybersecurity Risk Manager** - Dedicated to identifying, assessing, and mitigating risks to information security (Fig. 3).
4. **Cyber Threat Intelligence Specialist** - Specializing in gathering and analysing threat intelligence to inform defensive strategies (Fig. 4).
5. **Cybersecurity Educator** - Aiming to teach and promote cybersecurity awareness and best practices within organizations (Fig. 5).
6. **Cybersecurity Auditor** - Focused on evaluating and improving an organization's cybersecurity policies, practices, and controls (Fig. 6).

7. **Digital Forensics Investigator** - Specializing in the recovery and investigation of material found in digital devices, particularly relating to cyber crimes (Fig. 7).
8. **Incident Responder** - Concentrating on managing and responding to cybersecurity incidents to minimize damage and recover operations effectively (Fig. 8).

This targeted approach allows students to gain in-depth knowledge and skills tailored to their career aspirations in the rapidly evolving field of cybersecurity.

Fig. 1: A 120 ECTS Master's Program Preparing for the Role of *Chief Information Security Officer (CISO)* - Possible Pathway in a 2-Year Full Time Program

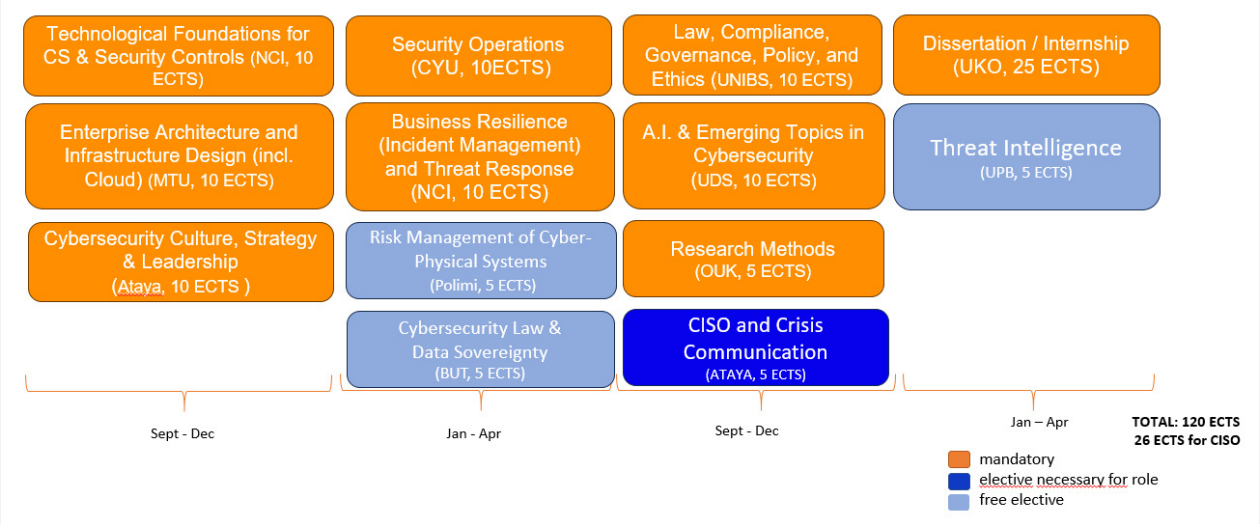


Fig. 2: A 120 ECTS Master's Program Preparing for the Role of *Cyber Legal, Policy, and Compliance Officer* - Possible Pathway in a 2-Year Full Time Program

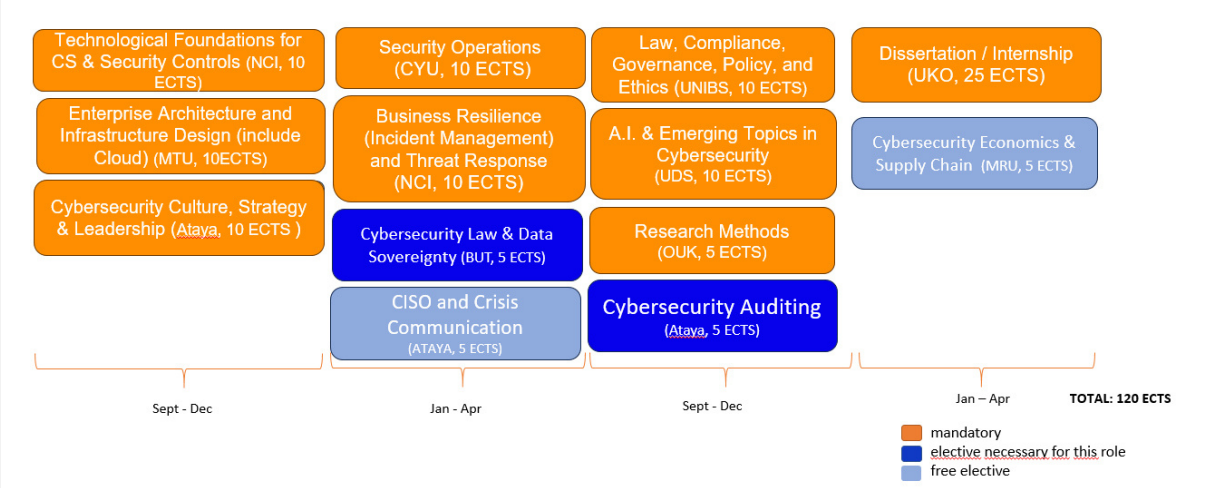


Fig. 3: A 120 ECTS Master's Program Preparing for the Role of *Cybersecurity Risk Manager* - Possible Pathway in a 2-Year Full Time Program

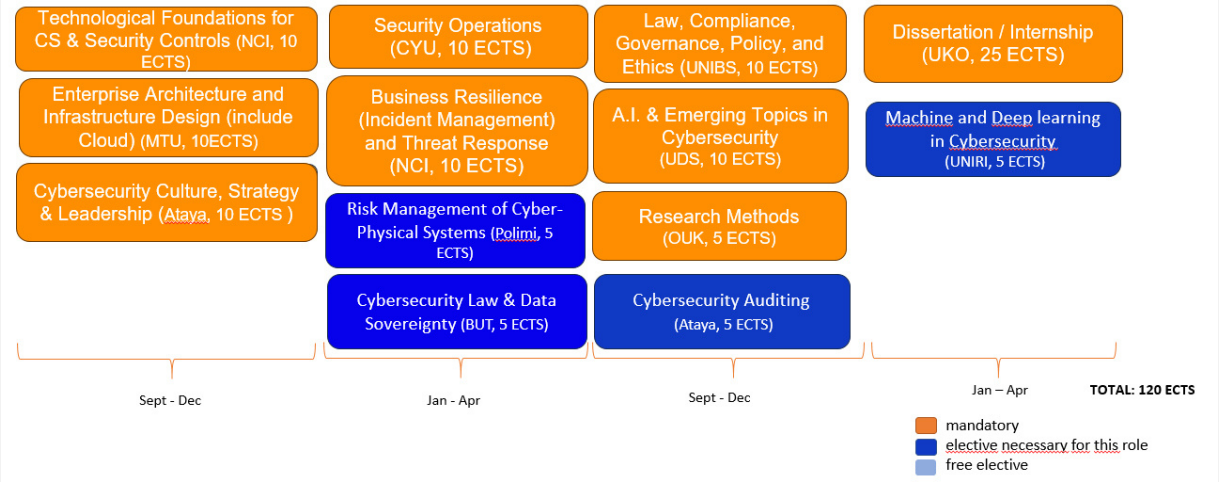


Fig. 4: A 120 ECTS Master's Program Preparing for the Role of *Cyber Threat Intelligence Specialist* - Possible Pathway in a 2-Year Full Time Program

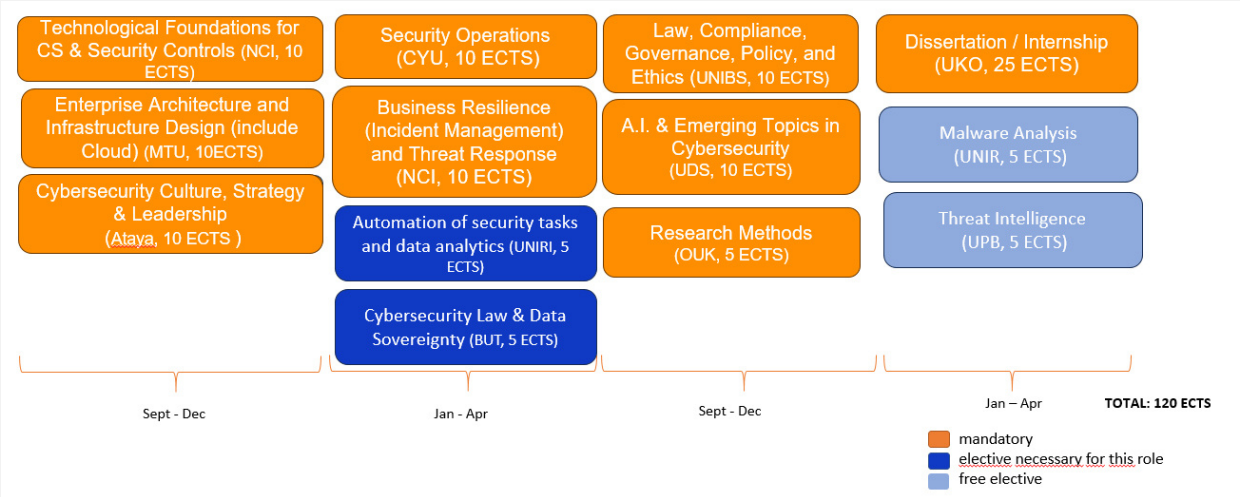


Fig. 5: A 120 ECTS Master's Program Preparing for the Role of *Cybersecurity Educator* - Possible Pathway in a 2-Year Full Time Program

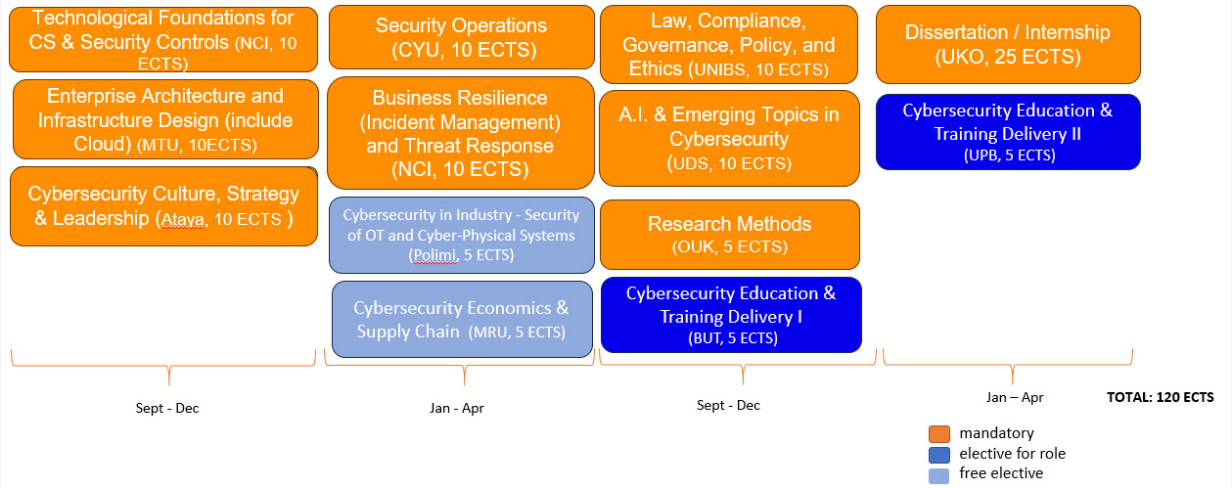


Fig.6: A 120 ECTS Master's Program Preparing for the Role of *Cybersecurity Auditor* - Possible Pathway in a 2-Year Full Time Program

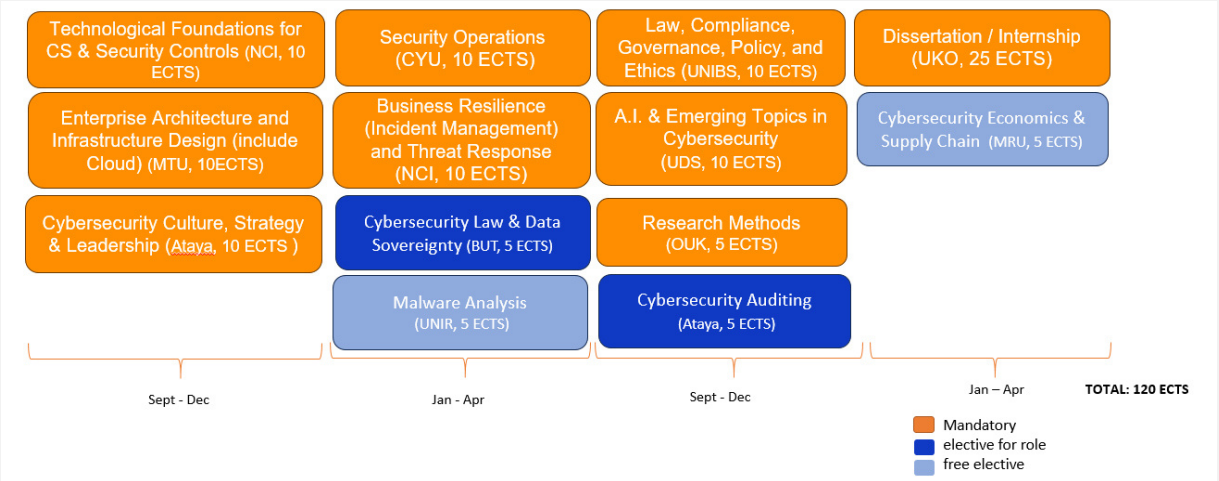


Fig. 7: A 120 ECTS Master's Program Preparing for the Role of *Digital Forensics Investigator* - Possible Pathway in a 2-Year Full Time Program

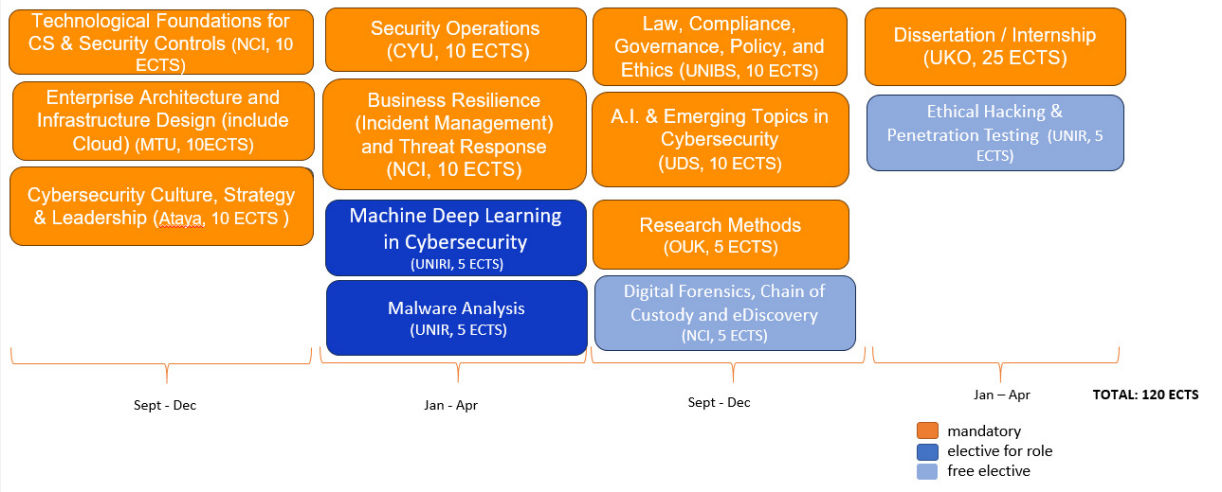
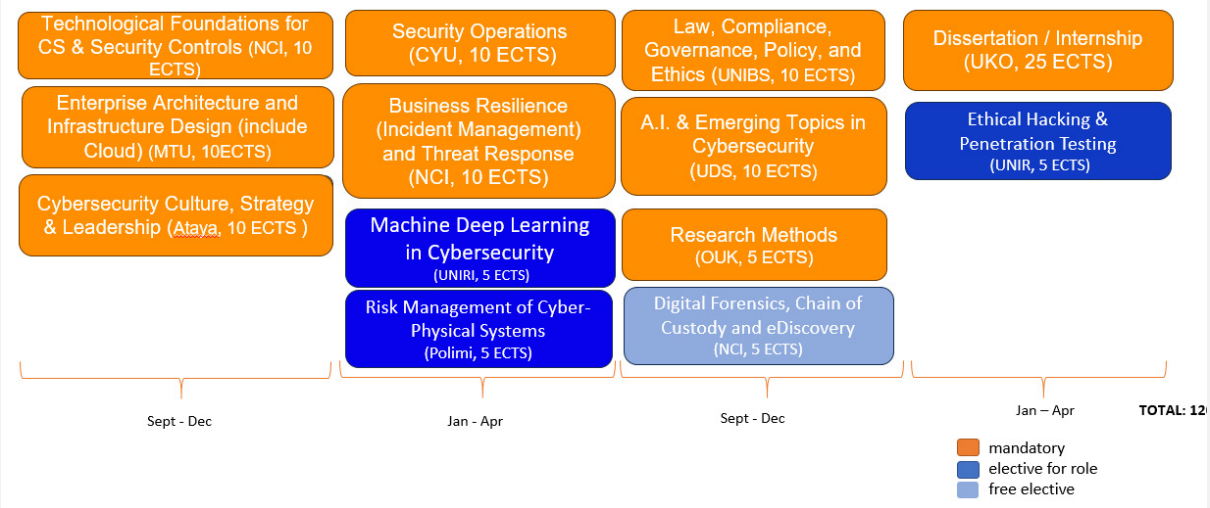


Fig. 8: A 120 ECTS Master's Program Preparing for the Role of *Incident Responder* - Possible Pathway in a 2-Year Full Time Program



The roles listed above are not classified as EU-regulated professions. While they are crucial within the cybersecurity field, they do not fall under formal regulation by the EU, meaning there are no specific legal requirements or regulatory bodies that govern who can perform these jobs.

However, the DIGITAL4Security program aligns closely with the European Cybersecurity Skills Framework. It ensures adherence to internationally recognized standards and certifications. To achieve this alignment, the program actively collaborates with industry experts and advisory boards comprised of professionals who hold certifications such as CISSP, CISM, and CTIA. This collaboration informs the curriculum design, ensuring that course content reflects the competencies required for these credentials. Furthermore, practical training modules are integrated into the program to prepare students for the certification examination processes associated with these qualifications.

Additionally, the program incorporates key regulatory frameworks, including the European Union General Data Protection Regulation (GDPR) and the European Cybersecurity Skills Framework (ECSF). This is achieved through dedicated coursework focused on data protection, compliance, and risk management practices, which are integral to maintaining regulatory standards in cybersecurity. By embedding these frameworks into the curriculum, students gain a comprehensive understanding of the legal and ethical considerations relevant to cybersecurity roles in Europe.

While the above profiles are not EU-regulated, the master's program is set to integrate industry certifications, leveraging strategic partnerships with key IT sector leaders. The program expects to offer industry certifications through Advanced Professional Microsoft Certificates and role-based certification programs. Students shall have access to the necessary infrastructure for certification, including localized testing centers and online certification options.

Certifications will be embedded into the curriculum at key milestones to complement academic learning. Students will participate in preparatory training sessions led by industry experts, followed by certification exams in areas such as Advanced Professional Microsoft Certificates, Security, Compliance, and Identity, or specialized cybersecurity tracks. The exams will be proctored either in-person at designated centers or remotely, ensuring flexibility for full-time and part-time students. This certification process shall be rolled out in three stages:

1. **Preparation**: Academic partners will provide study materials, tutorials, and mock exams to prepare students for industry certification tests.
2. **Examination**: Exams shall be delivered through both physical and virtual testing environments, ensuring accessibility across the partner countries.
3. **Certification**: Upon passing, students will receive industry-recognized credentials alongside their academic degree, validating their skills for the job market.

The module descriptions are currently under review. Based on each module's learning outcomes and content, a suite of recommended industry certifications will be identified, with testing options made available to students after completing the respective courses. Each module is being assessed to determine the extent to which its content covers the knowledge, skills, and competencies required for a particular industry certification exam. If a module covers approximately 80% of the required material, self-study resources shall be provided for the remaining 20%. This approach aims to ensure that no additional burden is placed on instructors, as they are not required to modify their existing materials or course plans. Of course, instructors have the option of expanding their materials, so that in some cases all relevant content may be covered in class. Students will also be granted access to practice tests for self-assessment before registering for official certification exams.

Regarding the testing setup, the existing infrastructure at HEIs and industry partners is being reviewed to minimize financial and time investments for offering in-person testing options. For online testing, we are exploring the feasibility of using Moodle, the current platform for course delivery and academic testing, as a preferred solution for industry certification exams. For the technical issuance of certificates, the consortium plans to utilize Full Fabric, which has been selected and implemented as the Customer Relationship Management (CRM) system for the master's program. This technical setup ensures that industry certifiers issue certificates through a standardized process, verifying that students have met the necessary requirements. Thus, Full Fabric is foreseen as a central system for managing and distributing certifications for both industry and academic purposes.

7. Different Accreditation Models

Similar to industry certification, various models for academic accreditation have been considered to determine the most suitable approach for launching the Master's Programme in Cybersecurity Management and Data Sovereignty. The following options provide a comprehensive overview of possibilities, enabling well-informed strategic decisions.

European Approach for Quality Assurance of Joint Programmes

This approach is specifically designed for joint programs and allows a single accreditation process for all Higher Eduction Institutions (HEIs).

- **Estimated Cost**: Approx. €20,000–€35,000, depending on the accreditation agency and specific requirements.
- **Advantages**:
    - A single accreditation for all HEIs.

  - It can simplify recognition across the European Higher Education Area (EHEA).
  - Aligned with Bologna principles and EQAR-registered agencies
- **Disadvantages**:
  - Complexities may arise in aligning diverse national requirements.
  - A high amount of consorted effort is required from all HEIs, as the accreditation outcome hinges on the quality and timely contribution of each partner.
  - The process is still relatively new, and therefore the practical implementation might not yet be fully streamlined or standardized across all contributing stakeholders.
- **Timeline**:
  - Typically 6–18 months from initial application to final decision, though speed-procedures reducing the process to just a few months are possible.
- **Fastest and Most Reliable?**
  - Relatively fast and reliable if all HEIs operate within the EHEA and have compatible regulations.

National Accreditation Processes in Each Country

Each HEI secures accreditation for its portion of the program through its national authority.

- **Estimated Cost**: Varies significantly, but can range from €5,000–€20,000 per institution.
- **Advantages**:
  - Tailored to national requirements, ensuring compliance in each jurisdiction.
  - May leverage existing accreditation processes at each HEI.
- **Disadvantages**:
  - Duplication of effort across institutions.
  - Higher overall costs and administrative burden.
  - Potential inconsistencies in quality standards across countries.
  - There is no accreditation of the master's programme at large.
- **Timeline**:
  - May require one to three years, as national processes can require substantial review time.
- **Fastest and Most Reliable?**
  - Not ideal for speed; only reliable if institutions have pre-existing accreditation workflows and national processes are fast.

Modular Accreditation for Microcredentials

Instead of accrediting the full program, individual modules or clusters of modules are accredited as **microcredentials**.

- **Estimated Cost**: €2,000–€10,000 per module or cluster.

- **Advantages**:
  - Allows HEIs to launch components of the program while full accreditation is in progress.
  - Modular approach enables flexibility and adaptability.
  - Easy recognition through ECTS framework.
- **Disadvantages**:
  - Does not lead to a full master's degree unless modules are later aggregated under a unified accreditation.
  - Limited appeal to students seeking a full degree.
- **Timeline**:
  - 6–12 months per module.
- **Fastest and Most Reliable?**
  - Fast and scalable for immediate offerings, but full program recognition may be delayed.

Joint or Double Degree Accreditation

Each HEI is responsible for accrediting its portion of the program, with a joint or double degree awarded.

- **Estimated Cost**: €15,000–€50,000 overall, depending on the scope.
- **Advantages**:
  - Allows each HEI to issue its degree, which may have better national recognition.
  - Less dependence on a unified framework.
- **Disadvantages**:
  - Complex administrative coordination.
  - Students may find the structure confusing or less attractive.
- **Timeline**:
  - 12–24 months for full implementation.
- **Fastest and Most Reliable?**
  - Moderate in speed and reliability, depending on inter-institutional agreements.

European or International Professional Body Accreditation

Seek accreditation from cybersecurity-specific organizations such as (ISC), ISACA, or ENISA.

- **Estimated Cost**: €10,000–€25,000, depending on the organization and program size.
- **Advantages**:
  - Adds industry recognition, enhancing employability.
  - Streamlined process compared to traditional academic accreditation.
- **Disadvantages**:
  - Not equivalent to formal academic accreditation.

  - May need additional steps to achieve degree recognition.
- **Timeline**:
  - 6–12 months.
- **Fastest and Most Reliable?**
  - Fast and industry-relevant, but lacks full academic weight.

Accreditation through European Microcredential Framework (EMCF)

Apply for recognition of individual modules or the entire program under the European Microcredential Framework.

- **Estimated Cost**: €5,000–€15,000.
- **Advantages**:
  - Quick pathway to launch modular programs.
  - Facilitates stackable learning, enabling students to gradually earn a full degree.
- **Disadvantages**:
  - Limited immediate recognition as a master's degree.
  - Requires follow-up accreditation for the full program.
  - The process is still relatively new, and therefore the practical implementation might not yet be fully streamlined or standardized across all contributing stakeholders.
- **Timeline**:
  - 6–9 months for initial recognition.
- **Fastest and Most Reliable?**
  - Fast for modular deployment, but not suitable for immediate master's recognition.

Table 5 presents an overview of these options.

Table 5: A Comparison of Academic Accreditation Models

Option	Estimated Cost (€)	Timeline	Advantages	Disadvantages
European Approach	20,000–35,000	6–18 months	Unified, EHEA-compatible	Requires multi-country alignment
National Accreditation	5,000–20,000/HEI	18–36 months	Tailored to each HEI	Duplication of effort
Modular Accreditation (Micro-credentials)	2,000–10,000/module	6–12 months/module	Fast, flexible for components	No immediate full degree
Joint or Dual Degree	15,000–50,000	12–24 months	National-level acceptance	Administrative complexity

Professional Body Accreditation	10,000–25,000	6–12 months	Industry-recognized	Not academic accreditation
EMCF	5,000–15,000	6–9 months	Quick, stackable	Not a full master's degree upfront

7.1 Selected Academic Accreditation Model: The European Approach for Quality Assurance of Joint Programmes

The European Approach for Quality Assurance of Joint Programmes has been selected as the preferred method for accrediting the entire Master's programme, as it best aligns with the D4S consortium's vision of realizing European collaboration across nations and institutions. Additionally, accreditation of micro-credentials is being envisioned to facilitate a modular rollout of the courses, allowing for pilot testing and supporting the scalable delivery of the full programme.

Requirements and Criteria of the Selected Accreditation Model

The **European Approach for Quality Assurance of Joint Programmes** establishes comprehensive criteria and standards for ensuring the quality and effectiveness of joint higher education programmes within the European Higher Education Area (EHEA). The eligibility requirements for participating institutions include recognition by relevant authorities in their respective countries and compliance with national legal frameworks that allow for joint programme participation and the awarding of degrees. Institutions must work collaboratively in designing and delivering the programme, with clear roles and responsibilities outlined in a cooperation agreement that covers aspects such as degree denomination, financial arrangements, student admission, mobility, and assessment procedures.

In terms of learning outcomes, the intended outcomes must align with the corresponding level in the Framework for Qualifications in the EHEA and applicable national qualifications frameworks. These outcomes should reflect the knowledge, skills, and competencies relevant to the disciplinary field, and the programme must demonstrate that these outcomes are achieved. In cases involving regulated professions, the programme must consider minimum training conditions specified in relevant EU directives.

The study programme should be structured to enable the achievement of the intended learning outcomes, with a clear application of the European Credit Transfer System (ECTS). The total student workload for joint bachelor programmes typically ranges from

180-240 ECTS, while joint master programmes typically require 90-120 ECTS, with a minimum of 60 ECTS at the second cycle level. The workload and completion time should be monitored throughout the programme.

Admission requirements and selection procedures must be appropriate for the programme's level and discipline; recognition of qualifications and study periods must align with the Lisbon Recognition Convention. Teaching and learning approaches must correspond with the intended learning outcomes, and the diversity of students should be respected, particularly considering their varied cultural backgrounds. Assessment procedures should be consistent among partner institutions and aligned with the learning outcomes.

Student support services must contribute to achieving the intended learning outcomes and address the unique challenges faced by mobile students. Adequate and qualified staff, with professional and international experience, should be available to implement the programme. Facilities should also be sufficient to meet the needs of the programme and the intended learning outcomes.

Transparency is crucial, with clear documentation on admission requirements, assessment procedures, and other programme details made readily available. Finally, participating institutions must apply joint internal quality assurance processes in line with the European Standards and Guidelines (ESG), ensuring continuous improvement and compliance with the established quality criteria.

Further details are provided by:
https://www.eqar.eu/kb/joint-programmes/agreed-standards.

The European Approach for Quality Assurance of Joint Programmes is further explored in section 10 below, examining both the political objectives and practical considerations involved in the implementation.

Prototype Accreditation Procedure with VLUHR QA

Designing a pan-European master's programme is a complex undertaking, and while several of the D4S deliverables have been postponed, the consortium has decided to generally maintain D3.3, implementing a prototype accreditation procedure in 2024 to accelerate learning and project progress. It is important to note that the deliverable of D3.3 is a demonstrator, pilot, or prototype, with the accreditation process otherwise covered in T6.1. However, implementing a real accreditation procedure at this point offers key advantages in terms of accelerating progress:

- The procedure requires the compilation of all relevant documents, addressing the quality standards and criteria outlined in the accreditation approach. This process

sheds light on all the details that need to be finalized, fast-tracking consortium discussions and decisions.
- The approach draws attention to national regulatory frameworks, enabling project partners to engage in concerted outreach to collect all necessary insights.
- The approach provides an ideal learning opportunity by facilitating concrete assessments from the accreditation panel and agency. Even if the outcome is a non-compliant result, the procedure highlights specific gaps that need to be filled, facilitating targeted completion.

At this point, the likelihood of achieving a fully-compliant accreditation verdict seems limited for two key reasons:

- With other project deliverables delayed, several details and the overall progress of the master's programme are not as advanced as would typically be desirable in programme accreditation.
- For the accreditation prototype to occur in 2024, a highly time-compressed procedure must be implemented. This required compiling accreditation documents and responding to panel assessments under extreme time pressure, leaving the consortium with limited opportunities for discussion, collaborative work, and careful content production.

Despite these challenges, this approach has been chosen because it promises the best opportunities to fast-track the entire project and master's programme, ensuring the quickest and most effective progress possible under the current circumstances. While probabilities are limited, there is also a slight chance that the programme could obtain immediate accreditation, enabling the fastest possible rollout. Against this background, different quality assurance agencies were contacted in July 2024. However, only one positive response was received, from VLUHR QA, while feedback from other agencies indicated no capacity to support such a fast-track procedure. The pricing model of VLUHR, at €34,900, reflects the demands of this accelerated procedure.

The timeline for the accreditation process is outlined in Figures 9 and 10.

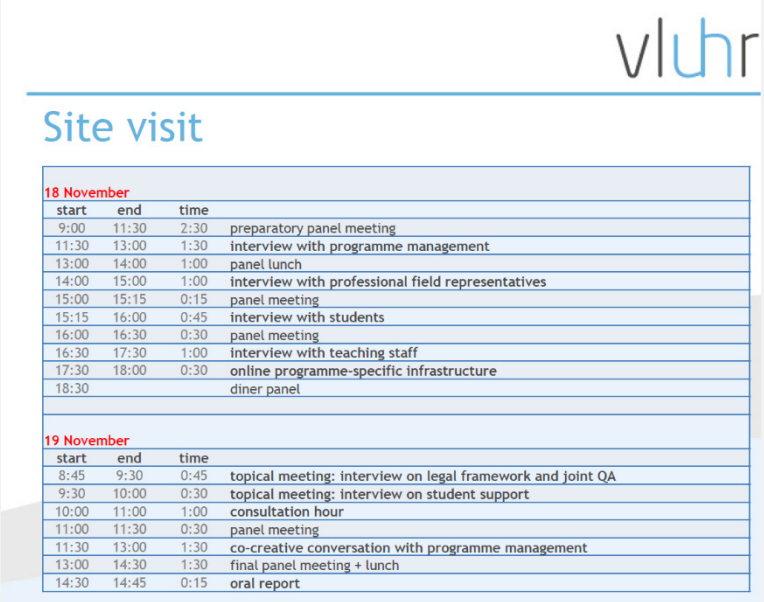
Figure 9: The accreditation timeline agreed upon with VLUHR, starting with initial exchange in July '24, and the actual procedure commencing in October '24.

Figure 10: The accreditation timeline agreed upon with VLUHR, concluding by the end of December '24, thus outlining an actual accreditation process over 3 months, with a prolonged timeline including preparatory meetings spanning six months.

On October 11, VLUHR met with D4S representatives to explain their expectations for the accreditation documents. The deadline for submission was extended from October 17 to October 25. The documents were subsequently compiled and submitted.

On November 18 and 19, an expert panel evaluated the master's programme during a site visit in Bucharest, with representatives from all involved higher education institutions present. The agenda of this meeting is provided in Figure 11.

Figure 11: The agenda of the accreditation site visit, where the panel interviewed various program representatives, including program management, industry experts, students, and teaching staff.



vluhr

Site visit

18 November

start	end	time	
9:00	11:30	2:30	preparatory panel meeting
11:30	13:00	1:30	interview with programme management
13:00	14:00	1:00	panel lunch
14:00	15:00	1:00	interview with professional field representatives
15:00	15:15	0:15	panel meeting
15:15	16:00	0:45	interview with students
16:00	16:30	0:30	panel meeting
16:30	17:30	1:00	interview with teaching staff
17:30	18:00	0:30	online programme-specific infrastructure
18:30			diner panel

19 November

start	end	time	
8:45	9:30	0:45	topical meeting: interview on legal framework and joint QA
9:30	10:00	0:30	topical meeting: interview on student support
10:00	11:00	1:00	consultation hour
11:00	11:30	0:30	panel meeting
11:30	13:00	1:30	co-creative conversation with programme management
13:00	14:30	1:30	final panel meeting + lunch
14:30	14:45	0:15	oral report

Afterward, on December 5, the D4S consortium received a report with preliminary evaluations from the accreditation panel. The consortium then had until December 9 to submit responses, such as clarifications or additional context. The panel sent their final assessments by December 13.

VLUHR has emphasized that at this point all assessment information is preliminary and confidential. Therefore, it is not included in this report. Generally, the assessments serve to pinpoint aspects of the programme that require finalization, providing clear guidance for the consortium's next steps. In the event that the current assessment result is a non-compliant outcome, a new accreditation process can be initiated at any time, based on the existing documents, which would only require incremental refinements. The current accreditation documents, which represent a highly refined prototype, are attached as Annex I to this report and include the following documents:

- Self Evaluation Report (SER)
- Cooperation Agreement

- Module Handbook
- Study and Examination Regulations
- Academic Staff CVs
- Internal Quality Handbook
- Student Handbook
- Sample Degree Certificate
- Sample Diploma Supplement
- Sample Evaluation Questionnaires

Timeline Considerations

As part of the accreditation prototype procedure, information has been collected on timeline requirements. Three subsequent phases need to be considered:

Cooperation Agreement Review: The Cooperation Agreement, which is part of the accreditation documents, must undergo review by the legal offices of all participating HEIs. Experience shows that this process typically takes at least 1-2 months. In the case of our prototype procedure, some universities were unable to get the Cooperation Agreement signed in time for the fast-tracked procedure, raising concerns during the accreditation assessment.

Accreditation Review: The actual accreditation review takes a minimum of 3 months. In our prototype procedure, the contract with the agency was signed in early October 2024. Expectations for document submission and the overall process were communicated immediately thereafter by the agency. This ongoing process is anticipated to conclude by the end of December 2024.

However, such an expedited timeline comes at the cost of somewhat reduced accreditation probability. The consortium had minimal time to compile the necessary documents, limiting opportunities for thorough deliberation, discussion, partner familiarization with key points, and coordinated decision-making. For instance, the consortium was given only two working days to process the initial panel assessment, identify and address errors, and draft a joint response letter - steps that typically span several weeks in standard accreditation procedures.

While fast-tracking can accelerate bringing the master's program to market, the likelihood of successful accreditation diminishes due to the compressed timeline, which constrains the consortium's ability to produce high-quality materials. This challenge is particularly acute when accreditation documents must be created from scratch, as opposed to refining existing materials, which is more feasible under time pressure.

Nevertheless, the learning and progress achieved are significantly accelerated by conducting an actual accreditation procedure, whether it follows a fast-tracked or more standard schedule.

National Accreditations: Under the European Approach for Quality Assurance of Joint Programmes, the intent is to offer a single accreditation process, designed to ensure compliance with shared European standards. However, national frameworks in participating countries still require additional steps to formally recognize the EU-level accreditation.

To better understand these national requirements, we conducted a survey among partner HEIs on the typical duration of national procedures following European-level accreditation. The results, presented below, indicate that a significant portion of the overall accreditation timeline may be consumed by these national steps, which can take half a year or longer (see Fig. 12).

The programme can only roll out once all degree-awarding partners are legally authorized to enroll students and issue degrees. Section 10 discusses the implications of this regulatory situation and considers future prospects for streamlining accreditations under the European framework.

Fig. 12: Following the programme's successful EU-level accreditation, national approvals must be secured. A survey among academic partners highlights the expected duration of these national accreditation procedures, which significantly extend the overall accreditation timeline.

	Expected Duration of National Accreditation
Romania	2 months
Ireland	6 months +
Germany	max. 3 months
Croatia	2-3 months
Italy	3 months / 6 months*
Lithuania	2 months / 12 months +*
Spain	No timeframe reported.
	*different partners reporting different timelines

The consortium plans to initiate another accreditation process in early 2025, following the European Approach for Quality Assurance of Joint Programmes, should the current process receive a non-compliant evaluation. With a comprehensive set of accreditation documents already in place, the feedback from the ongoing review will help identify and address any issues swiftly. This targeted progress aims to ensure the quickest possible rollout of the master's programme while meeting all accreditation requirements. Additionally, the standards of the European Approach have been endorsed internally, with the consortium adopting an aligned programme management structure and quality assurance procedures (sections 8 and 9).

7.2 DIGITAL4SECURITY MASTER'S GOVERNANCE AND MANAGEMENT STRUCTURE

For the accreditation process and the implementation of internal quality assurance mechanisms within the program, it has been crucial to define governing bodies that extend beyond the scope of the EU project to ensure the program's long-term sustainability. These bodies play a pivotal role in implementing the quality assurance mechanisms detailed in the subsequent section. A clear definition of these governance structures is indispensable for accreditation, as they must be explicitly outlined in the Cooperation Agreement and supporting annexes of accreditation documents.

The D4S Consortium has agreed upon the following bodies and is currently in the process of nominating the individuals holding specified roles.

Programme Directors
Each Partner Institution appoints one academic Programme Director responsible for ensuring alignment between the local program implementation and joint agreements. Programme Directors collaborate with counterparts from other institutions on all program matters.

Programme Coordinators
Programme Coordinators support Programme Directors by handling daily administrative and technical tasks related to students, quality assurance, and program delivery. They collaborate with Programme Directors, other Coordinators, students, and external partners to enhance program quality and implementation.

Programme Faculty
Academic teaching staff from Partner Institutions and associated partners contribute to the development and delivery of the program.

Issuing Institution
This institution is responsible for awarding the joint degree and its supplementary documentation, in coordination with all degree-awarding and non-degree-awarding Partner Institutions.

Project Coordinator
The Coordinator oversees:

- Student recruitment, onboarding, and support.
- Implementation of industry certifications and micro-credentials.
- Establishment of employability and European mobility programs.
- Faculty training resources.

The program governance furthermore includes several joint bodies responsible for various aspects of the degree program:

Master's Board of Directors
Comprised of Programme Directors from each Partner Institution, the Board oversees general management, quality assurance, financial supervision, and academic matters. It meets at least twice a year.

Programme Secretariat
Based at the Project Coordinator Institution, the Secretariat manages daily operations, quality assurance, student administration, and mobility coordination. It also supports the Master's Board and maintains program documentation.

Joint Admissions Board
Responsible for selecting and admitting students, the Board consists of representatives from each Partner Institution and convenes after application deadlines.

Examinations Board
Overseen by the Master's Board, this body ensures academic standards and quality across the program. It meets after examination sessions to deliberate and resolve cases as needed.

Joint Programme Committee
This body advises the Master's Board on policy and system reviews to maintain program coherence and consistency. It meets annually or as required.

Quality Enhancement and Curriculum Development (QECD) Committee
This committee drives quality enhancement and curriculum development, aligning with European Standards and Guidelines. It evaluates learning objectives and proposes improvements.

Ad-hoc Committees
The Master's Board may establish temporary committees for specific assignments beyond the scope of existing bodies.

7.3 Quality Assurance Procedures

The consortium has adopted guidelines aligned with the European Approach for Quality Assurance of Joint Programmes, forming a key part of our Certification Standards Catalogue alongside other documents in Annex I, such as the Study and Examination Regulations. These guidelines, along with the endorsed procedures and governance bodies, support the design, implementation, and evaluation of the master's programme, ensuring high quality and alignment with recognized European standards.

Procedures are in place to ensure regular content updates, following each Master's cycle. Procedures have also been prepared for collecting student feedback through regular surveys, to inform recommendations for updates in the program design and delivery. Annual

surveys of industry partners are also part of the Quality Assurance Plan. Further details on these surveys can be found in the Sample Evaluation Questionnaires in Annex I.

The selected procedures are fully aligned with European accreditation requirements, particularly for Joint Degrees, and are detailed in the D4S Internal Quality Handbook (IQH) included in Annex I.

Overall, the following procedures have been defined:

- IQH.01 Procedure for Academic Performance Analysis
- IQH.02 Procedure for the Student Module Satisfaction Survey
- IQH.03 Procedure for Survey-Based Complementary Quality Management
- IQH.04 Procedure for Class Representative Meetings
- IQH.05 Procedure for Suggestions and Complaints
- IQH.06 Procedure for Quality Enhancement Planning

The outputs from Quality Assurance procedures are incorporated into an Annual Programme Review Report.

IQH.01 Procedure for Academic Performance Analysis

Internal Quality Procedure Reference	IQH.01
Title	Procedure for Academic Performance Analysis
Data Collection System	Each September, the Digital4Security Secretariat generates reports from the central administration system to assess cohort indicators for both Full-Time and Part-Time programmes. These include data such as (i) students who began each programme instance, (ii) current enrolment status in each programme, (iii) enrolment numbers for each module within both programmes.
Data Analysis System	The Project Coordinator and the QECD Committee analyse the academic performance indicators, diagnose possible causes for deviations from reference values and send an analysis report and improvement recommendations to the Master's Board of Directors in November.
Enhancement System	In November, the Master's Board of Directors considers the recommendations and delegates implementation of the enhancement measures to the Project Coordinator or specific partner institutions, unless decided otherwise.

IQH.02 Procedure for the Student Module Satisfaction Survey

Internal Quality Procedure Reference	IQH.02
Title	**Procedure for the Student Module Satisfaction Survey**
Data Collection System	Each term, the Secretariat distributes online surveys to student cohorts to gather feedback on their enrolled modules. Surveys are typically conducted in the second half of the teaching term, but before final exams. The module satisfaction survey covers subjects like course content, structure, workload relative to ECTS credits, practical applications, communication effectiveness, and inclusivity. Students have two weeks to complete the survey. The Secretariat processes survey responses within three weeks, supported by the QECD Committee. Results are compiled separately across the Full Time and Part Time programmes. They are summarized in a report shared with the Project Coordinator and Joint Programme Committee. Lecturers receive feedback on the modules they taught within two weeks of survey completion.
Data Analysis System	Annually, the QECD Committee monitors programme performance and prepares an Annual Programme Review Report summarizing key data, findings, and recommendations. This report is reviewed by the Master's Board of Directors, which may identify strategic adjustments. Lecturers review feedback on their modules to identify potential areas for improvement per teaching term.
Enhancement System	Based on the Annual Report, the Master's Board of Directors determines and delegates improvement measures to the Project Coordinators, QECD Committee, or partner institutions as needed. Lecturers use module-level feedback to explore alternative pedagogical strategies, if applicable, to enhance module delivery.

IQH.03 Procedure for Academic Performance Analysis

Internal Quality Procedure Reference	IQH.03
Title	**Procedure for Survey-Based Complementary Quality Management**
Data Collection System	The Secretariat distributes online surveys to various stakeholders to gather feedback. These typically include the following and can be selected based on guidance by the Master's Board of Directors in line with strategic objectives. ***(I) Student Feedback:*** In addition to the Module Satisfaction Survey (IQH.02), students are invited to provide feedback on their online learning experience, typically once during their first year and again in their final year of study. Feedback sections include the overall online study platform, navigation and usability, as well as the online learning experience. ***(II) Lecturer Feedback:*** After each module, or based on demand determined by the Master's Board of Directors, lecturers can be invited to provide feedback covering general module reflections, online teaching modality, student involvement and inclusivity, learning materials and tools, balance of practical vs. theoretical content, interaction and support, as well as feedback on the assessment process and grading. Additional feedback can be gathered on the appropriateness of assessment tasks for master's level, alignment with program learning outcomes, as well as the objectivity, reliability, and validity of grading, next to the completeness of topic coverage comparing the module content with assessment tasks. ***(III) Industry Expert Feedback:*** The industry expert survey is conducted regularly, such as once annually, aiming to collect at least two independent reviews per module, focusing on relevance to industry needs, content quality, inclusion of current issues and technologies, practical applications, and overall module assessments. Survey recipients have two weeks to complete the questionnaires.
Data Analysis System	The Secretariat processes survey responses within three weeks, supported by the QECD Committee. Performance is assessed, and findings are summarized in the Annual Programme Review Report, suggesting potential improvement measures.

	The Master's Board of Directors reviews this report to identify strategic adjustments and coordinates implementation with relevant bodies.
Enhancement System	The Master's Board of Directors decides on improvement strategies based on summary results from surveys as well as recommendations in the Annual Programme Review Report by the QECD Committee, delegating the implementation of improvement measures to the Programme and Project Coordinators, the QECD Committee and/or specific partner institutions, unless decided otherwise.

IQH.04 Procedure for Class Representative Meetings

Internal Quality Procedure Reference	IQH.04
Title	**Procedure for Class Representative Meetings**
Data Collection System	For each programme instance, during programme orientation, each cohort of students elects up to two individuals to act as class representatives. The role of the class representative is to serve as a formal interface between cohorts of students and the teaching and administrative staff for issues that may potentially have an impact at the group level. The Master Secretariat establishes communication channels with the class representatives for each cohort at the beginning of each semester. In the sixth week of each semester, class representatives are requested to submit documented feedback on various aspects of their program, such as academic content, student services, timetabling, and any concerns or positive points they wish to raise. We then inform the representatives that a meeting is scheduled for the eighth week, where they, along with the Master's Board of Directors and the Project Coordinator, will discuss this feedback and address any arising issues. In the virtual environment, class representatives are elected via an online voting platform. Nominations are collected through the learning platform or email, and students vote anonymously in a secure online poll during the orientation period.

Data Analysis System	On receipt of the class representative feedback for each cohort, the Master Secretariat forwards the feedback documentation to the Master's Board of Directors and the Project Coordinator. A meeting is then scheduled (for week 8) with the class representatives, the Master's Board of Directors, and the Project Coordinator. The Master's Board of Directors and the Project Coordinator consider the feedback provided by the class representatives. A set of responses is compiled addressing any issues raised for discussion at the scheduled week 8 meeting.
Enhancement System	The Master's Board of Directors, and the Project Coordinator discuss any issues raised by the class representatives at the scheduled week 8 meeting. Potential improvement proposals are also discussed, and a set of actions and tasks are compiled as an output of the meeting. These actions and tasks are the responsibility of the Project Coordinator who then delegates completion of the tasks to the appropriate person(s) or groups.

IQH.05 Procedure for Suggestions and Complaints

Internal Quality Procedure Reference	IQH.05
Title	**Procedure for Suggestions and Complaints**
Data Collection System	Students wishing to suggest or comment about the programme policies or services, either academic or non-academic, can do so informally: • at the university by contacting the person in charge (where it seems appropriate), • by raising non-individual matters with the student class representatives • by raising individual matters with their student advisor or tutor. If informal channels do not suffice, formal suggestions and complaints can be submitted: • by sending a message to either a representative of the Master Secretariat or the Project Coordinator,

	• by writing a formal letter to the relevant Programme Director and/or joint Programme Coordinator, or if the complaint is lodged against the Programme Director and/or Joint Programme Coordinator, by writing to the President of the Project Coordinator's institution.
Data Analysis System	The addressee of a complaint will keep the name of the issuer or any other reference anonymous (unless the complainer states otherwise) and facilitate a prompt resolution of the complaint. • The Master's Board will consider complaints about academic judgments, and about matters to do with the student's course of study or research, only if the candidate is not satisfied with the outcome reached by the partner institution associated with the module for which there is a complaint. • Regarding results of examinations the Board may function as a Review Committee only if the student is not satisfied with the outcome reached at the partner institution via interaction with the relevant Programme Coordinator. • Concerning the handling of complaints of academic judgments and the effective organization of tests and examinations the partner institutions guarantee a system that adequately takes into account the specific nature of the joint programme and its exigencies.
Enhancement System	An initial response to any complaint can be expected within 7 days of complaint receipt, and a considered response to the complaint should be received within a further three weeks, with any subsequent remedy implemented with the minimum of delay.

IQH.06 Procedure for Quality Enhancement Planning

Internal Quality Procedure Reference	IQH.06
Title	**Procedure for Quality Enhancement Planning**
Data Collection System	The QECD Committee decides on the organization of improvement actions that have been delegated to it by the Master's Board of Directors. The QECD Committee ensures that for every (major) improvement action a person is appointed as responsible for monitoring the improvement action during implementation and at completion. On completion, the appointed person creates an evaluation report which is made available to the Programme Coordinator, the QECD Committee and the Joint Programme Committee.
Data Analysis System	In cooperation with the Programme Coordinator, the QECD Committee compiles an overview report based on the improvement action evaluation reports. This is sent accompanied with recommendations for further action to the Board of Directors. These recommendations may include concrete proposals for modifications of the Internal Quality Handbook itself.
Enhancement System	The Master's Board of Directors adopts the recommendations and proposals and delegates their implementation to the Programme Coordinator, the QECD Committee and/or partner institutions involved, unless decided otherwise.

Further details of the planned Quality Assurance Mechanisms can be accessed in Annex I to this document, which provides our sample accreditation documents including extensively elaborated surveys for students, teaching staff and industry experts.

7.4 Reflections on the Accreditation Experiences of a Joint Master's Program in Europe

Based on the insights gained by the Digital4Security consortium, particularly in relation to academic accreditation, several crucial considerations have emerged that we would like to share at the European level.

We will begin by recapitulating the D4S project plan as defined in the Grant Agreement, reflecting the consortium's commitment to creating a European Master's program in Cybersecurity Management and Data Sovereignty. This program includes several features that seem clearly in Europe's interest, such as equipping SMEs and industries across Europe with essential cybersecurity skills as quickly as possible, offering a highly inclusive and accessible educational opportunity by hosting the program online, and connecting Europe's cybersecurity talent by offering the program collaboratively across European nations.

The European Approach to Quality Assurance for Joint Programmes appears, at first glance, to be ideally suited for supporting initiatives like ours. However, national regulatory landscapes have been slow to align with this European approach, causing significant challenges. For instance, some countries require on-site components, which conflicts with the program's envisioned fully online format. These regulatory complexities lead to compromises and delays, exposing a gap in understanding the realities of implementing the European Approach.

The core insights derived from the consortium's experiences highlight **structural dilemmas** that need to be addressed at the European level. Without political resolution, these dilemmas force difficult compromises, as ideal solutions in designing an attractive program conflict with practical accreditation requirements at the national level. Despite these hurdles, the consortium remains focused on delivering the highest-quality educational outcomes, emphasizing collaboration and transparency.

We invite EU guidance on which priorities to uphold in the face of conflicting goals. Overall, the consortium is eager to share its insights and is fully committed to intensifying exchanges, aiming to shape recommendations and help improve the broader European educational framework to ensure favourable conditions for implementing collaborative educational offerings across Europe.

The Aim of a Joint European Online Master's Program in Cybersecurity

The Digital4Security (D4S) consortium aims to address a critical digital skills gap in Europe by providing essential cybersecurity expertise to protect enterprises, infrastructure, and citizens. The Grant Agreement (Ares(2023)4917939 - 14/07/2023) states:

> **"**We will create an innovative and market-led **European Masters Programme in Cybersecurity Management & Data Sovereignty (DIGITAL4Security)** that will equip European SMEs and Companies across multiple sectors with the cybersecurity management, regulatory and technical skills they need to prevent and respond to existing and emerging cybersecurity threats, helping to safeguard European industries from cyber-attacks, protecting our economic prosperity, and supporting long-term competitiveness and growth" (Grant Agreement, p. 115, emphasis in original).

To maximize inclusivity and reach, the program prioritizes accessibility through an online format with no on-site requirements. This approach allows students to participate from anywhere in Europe, avoiding the need to relocate from rural areas to urban centres or from less developed regions to IT hubs. The Grant Agreement highlights the consortium vision to…

> "Create an **online** Masters Programme in Cybersecurity Management that will be **highly accessible**, affordable and convenient for the maximum number of students" (Grant Agreement, p. 81). It envisions the "Delivery of the **Online** European Cybersecurity Masters Programme" (p. 84, emphasis added).

Beyond this, the D4S consortium champions a European ideal of collaboration, uniting leading universities across multiple countries to offer a joint master's degree. With 37 partners from 13 countries, including 13 higher education institutions in nine European nations, it represents a pioneering network that aims to jointly advance pan-European education (see Section 1 above).

This extensive network represents a collaborative effort in education, jointly offering a master's degree on a pan-European scale. The consortium recognizes its role as a trailblazer in setting standards for European collaboration in designing joint educational formats. With this in mind, we aim to generate new knowledge on how to successfully implement such a program in Europe. The insights gained shall be shared with other consortia of European universities, supporting the creation of similar pan-European educational offerings. The Grant Agreement outlines…

> "the adoption of the D4S model as a best practice for other joint Masters programmes by HEIs and European University Initiatives. During the project we will **create a knowledge base** that will help us develop the programme and platform to **create a 'best practice' model that others can follow**. This will include **guidelines** on how to deliver the framework for other HEIs / EUIs" (Grant Agreement, p. 89f., emphasis added).

The Idea(l) of a European Approach to Quality Assurance of Joint Programmes

Aligned with the consortium's vision, the **European Approach for Quality Assurance of Joint Programmes (EAQAJP)** provides a framework for establishing pan-European degrees, such as the joint master's program developed by our 13 universities. Designed to unify and streamline the accreditation process, the EAQAJP aims to eliminate the need for separate national accreditations:

> "The present European Approach for Quality Assurance of Joint Programmes has been developed to **ease** external quality assurance of these programmes. In particular, it will [...] **dismantle an important obstacle** to the development of joint programmes by setting standards for these programmes that are based on the agreed tools of the EHEA, **without applying additional national criteria**" (EQAR documentation, ***European Approach for Quality Assurance of Joint Programmes***, approved by EHEA ministers in May 2015, p. 1, emphasis added).

If implemented as intended, the EAQAJP would provide an ideal foundation for a pan-European master's degree in cybersecurity by:

- **Supporting joint degrees across multiple nations**
- **Promoting the ideal of pan-European collaboration**
- **Ensuring a time-efficient approach**, which is critical for EU-funded projects like D4S expected to transition from early concept to self-sustaining practice within four years.

The potential efficiency of the EAQAJP can be demonstrated through the example of quality assurance processes in Germany. Ideally, an EAQAJP assessment would suffice, with no additional national criteria or extensive processing times required. This principle is explicitly stated by the German Foundation for Accreditation on behalf of the Accreditation Council:

> "The Accreditation Council **only checks whether an evaluation according to the European Approach (EA) has taken place**, meaning whether the program has been assessed based on the criteria and procedural rules of the EA.
> It **does not perform a secondary evaluation** of the program!" (Stiftung Akkreditierungsrat, 2023, p. 8, our translation and emphasis).

The German Accreditation Council, which convenes four times annually, has furthermore introduced measures to expedite decisions for EAQAJP-accredited programs. While typical processing times may extend up to three months, fast-tracking mechanisms allow for decisions between official meetings:

> "The Accreditation Council has delegated recognition decisions to the executive board, enabling **timely decisions** and ensuring that higher education institutions **do not need to consider the meeting dates** of the Accreditation Council." (Stiftung Akkreditierungsrat, 2023, p. 12, our translation and emphasis).

By removing significant administrative obstacles, the EAQAJP stands as a promising tool to facilitate the development and accreditation of joint master's programs across Europe.

Realities of a European Approach to Quality Assurance of Joint Programmes

Despite the ideal of a streamlined European accreditation process, national regulatory frameworks remain highly complex. Already in 2017, implementation difficulties regarding the European Approach to Quality Assurance of Joint Programmes (EAQAJP) led to the formulation of tailored recommendations for improving the procedure.

> "The PLA conference brought together [...] education ministries, quality assurance organisations, higher education institutions, and the European Commission and EACEA [...]. This report is based on their practical experiences with the European Approach, and their advice and considerations in the PLA discussions" (Becker, 2017, p. 2).

The report outlines concrete action points for key stakeholders, including:

Action Points for Ministries of Education

- "Include European Approach into the national legislation. Quickly.
  Follow-up with what has been agreed / confirmed / ratified by the EHEA education ministers [...]; map and cross-**check existing legislation - identify obstacles - introduce changes**." (p. 32, our emphasis)
- "Accept the verdict of a European Quality assessment. If an institution passes a European Quality assessment the university (of applied sciences) should be allowed to handout degrees **without additional (national) checks of accreditation bodies**." (p. 32, our emphasis)

Action Points for Quality Assurance Organizations

- "Explain the European Approach to HEIs. Identify differences between the EA and the national procedures and **make this info transparent to HEI**." (p. 33, our emphasis)
- "**Be more flexible and accept differences**, taking into account the fact that **it is a priority to propose such programmes** than not having them because they are not exactly in the frame of QAA." (p. 33, our emphasis)

Action Points for Higher Education Institutes

- "Unite [...] and request Ministries, Parliaments and QA agencies **to amend national legislation to allow for single accreditation of a joint programme**." (p. 33, our emphasis)
- "Continue to **mention the challenges faced**. Prepare well-justified **supporting documentation** and **case studies**, and submit to the Ministry of Education." (p. 33, our emphasis)
- "Remind their education ministries / legislators of **the promise** that the HEIs would be able to use the European Approach." (p. 33, our emphasis)

Action Points for the European Commission

- "**Reduce bureaucracy**, insert European accreditation in EC law." (p. 34, our emphasis)
- "**Listen to obstacles** of applicants wanting to use the EA and try to **help them**. Liaise with ENQA, EQAR, DG EAC." (p. 34, our emphasis)
- "**Provide funding to identify differences** between EA and regular national procedures of QAA, develop joint single accreditation mechanism" (p. 34, our emphasis)

These insights and recommendations closely align with the objectives of our consortium. Below, we provide a detailed account of the obstacles encountered and the decisions required to overcome them. One key issue deserves particular emphasis:

When national regulations are not updated and thus remain misaligned with the EAQAJP criteria, national rules take precedence in determining whether the program can legally enroll students and issue degrees in those countries. This undermines the vision of a unified and straightforward accreditation process across Europe.

This challenge arose at a significant scale in the case of our project for two primary reasons:

- **The size of our consortium**: With members from diverse European countries, we must navigate a broad spectrum of national regulatory frameworks.
- **The online nature of the program**: Many national regulations remain incompatible with the European Approach's allowance for fully online education, posing significant barriers to implementation.

Problem Assessment and Data Analysis

Within our consortium, intensive exchange took place among partners, their university legal offices, and national accreditation bodies. Based on this research, the consortium

concludes that Spain, Germany, Croatia, and Ireland can accredit a fully online master's degree under the European Approach. However, this is not the case for Romania, Lithuania, Italy, Czechia, and France, where additional requirements, including for on-site components, are currently mandated.

Furthermore, feedback on national processing times once the EAQAJP evaluation is available revealed that several countries require six or more months, with one partner reporting a 12-month timeline for issuing legal approvals. Additionally, several countries indicate uncertainties regarding their timelines. Importantly, the degree program can only be implemented once all degree-awarding partners have received legal approval to enroll students and issue the degree. This means the longest national timeline determines the earliest possible program start. Based on the data, a timeline of at least 8 months from EAQAJP results to the final national verdict appears realistic, or even optimistic (cf. Section 7 – Timeline Considerations).

Altogether, the **administrative processes** identified in this project suggest that **more than one year** is required between finalizing the program design and launching the program. These administrative procedures involve the following key steps:

Cooperation Agreement Processing: Review of documents by each university's legal office and signatures from all participating universities (1–2 months).

European Accreditation: Completing the EAQAJP process with a registered quality assurance agency (3–4 months).

National Accreditation: Securing permissions in all involved countries (approximately 8 months or more – depending on the nations involved and numbers of partners).

This means that at least one year - and likely more - must be accounted for between having the program fully developed and starting it with all required permits.

In our case, preparing the program for accreditation required compiling more than 430 pages of detailed documentation. Despite this extensive presentation, the accreditation panel still discussed areas calling for further elaboration. Importantly, the documentation of an intended master's program follows its actual design, including the development of teaching content, delivery methods, and envisioned governance structures. This design phase would typically be expected to be the most intensive phase of active project work, as prominently outlined in any program plan for launching a master's degree.

Against this background, it is clear that the original D4S proposal and Grant Agreement set an unrealistic timeline. The launch of an accredited master's degree program was planned for month 13, specifying the following deliverables (among others):

- **D4.1**: Full-time program over two years starting in M13.
- **D4.2**: Part-time program over three years starting in M13.

Based on the administrative insights gathered during this project, and as part of building an up-to-date knowledge base, it is clear that meeting the original timeline would have

required the entire master's program design and accreditation documents to be completed by the start of the project - or ideally, even earlier.

The original project timeline reflects a gap in understanding the complexities of accreditation processes across European countries. Our efforts contribute to the Grant Agreement's goal of creating a "knowledge base" (p. 89) for developing best practices.

The complexities of national regulations and their impact on timelines need to be investigated and shared across Europe. For instance, when our project proposal was initially submitted in the Digital Skills call, it received favourable reviews. Had more detailed data on accreditation timelines been available, the evaluations might have placed greater emphasis on discussing likely delays and hurdles in the proposed project plan.

Structural Dilemmas

The consortium encountered several structural dilemmas in aligning its project objectives with the Grant Agreement and the constraints of national accreditation processes. These dilemmas often forced the balancing of two equally valuable objectives, leading to challenging compromises. Those dilemmas highlight potential areas for policy improvement, particularly regarding structural and administrative conflicts. Insights from these experiences may also help other European consortia launching joint programs to anticipate such conflicts and prioritize strategic decisions early, thereby mitigating the impact of structural incompatibilities in accreditation and funding systems.

Conflicting Goals Yield Dilemmas

1. #### Accreditation Speed vs. Pan-European Inclusion
   The consortium faced a choice: either accelerate the accreditation process by limiting degree-awarding institutions to those "arbitrary" countries with streamlined administrative cycles and education policies that accept fully online formats, or pursue the ideal of pan-European inclusion. The latter approach would allow for the participation of more countries, but come at the cost of longer processing times and greater procedural uncertainties.

2. #### Online Format versus Leadership Mandates in the Grant Agreement
   A significant dilemma arose from the project's leadership being set to a country (Romania) that happens to be currently misaligned with the European Approach's allowance for fully online education. The consortium had to choose between maintaining the defined leadership role (in Romania), or fulfilling the commitment to a fully online program.

3. Taking on Educational Responsibility vs. Designing an Attractive Program
   The consortium unites nations dedicated to closing Europe's digital skills gap, with all members ready to take active roles, including leadership. However, structural barriers in national regulations force some countries (e.g., Romania, Lithuania, Italy, Czechia, and France) into a difficult choice: either adopt a passive role as mere "contributing partners" with limited responsibility and no leadership, or design alternative programs requiring a blended format with annual onsite attendance in arbitrary countries where such components are mandated. While the latter approach enables active participation by all countries, it produces less attractive programs that deviate from the Grant Agreement's vision of a fully online, highly accessible degree. This situation disproportionately disadvantages countries with slower regulatory adoption of European standards, confining their universities to passivity or the creation of second-tier programs.

Decision-Making, Compromises and Commitment to Excellence

The consortium engaged in thorough discussions to address the structural dilemmas faced during the project. While decisions were made typically by majority votes, dissenting voices raised concerns about deviations from the initial project vision. Despite these challenges, the consortium remained united in its commitment to delivering the European Master's Programme in Cybersecurity Management and Data Sovereignty to the highest quality standards. This commitment was accompanied by a willingness to make compromises in order to navigate the complexities of the regulatory landscape effectively.

Guidance and Facilitation by the EU

The consortium welcomes guidance from the EU on prioritization, particularly regarding the three structural dilemmas outlined above: which of the conflicting goals should take precedence in each case? Our ultimate objective is to offer the best possible program within a complex regulatory landscape, leveraging our collective expertise to overcome challenges and deliver transformative educational outcomes in cybersecurity for European learners and industries.

Fostering Collaboration and Transparency: From Insights to Recommendations

We also wish to emphasize our readiness to engage in policy communication, share learnings, and help in providing recommendations. We are committed to supporting the broader network of European universities, quality assurance agencies, education ministers, and the European Commission by offering transparent insights into the challenges we have encountered, as well as the lessons learned and actionable steps that can be derived from these experiences.

REFERENCES

Becker, R. (2019). *The European Approach for Quality Assurance of Joint Programmes*. Outcomes Peer Learning Activity, 5–6 October 2017, The Hague, Netherlands. Retrieved from https://www.erasmusplus.nl/sites/default/files/assets/Downloads/2017/ho/FABOTO/pla%20report%2031%2010%202017.pdf

Dow, S. P., Glassco, A., Kass, J., Schwarz, M., Schwartz, D. L. & Klemmer, S. R. (2010). Parallel prototyping leads to better design results, more divergence, and increased self-efficacy. *Transactions on Computer-Human Interaction, 17* (4), 18:1-24.

Dow, S. P., Heddleston, K., & Klemmer, S. R. (2009, October). The efficacy of prototyping under time constraints. In *Proceedings of the seventh ACM conference on Creativity and cognition* (pp. 165-174).

Dow, S.P. & Klemmer, S. R. (2011). The efficacy of prototyping under time constraints. In: H. Plattner, C. Meinel & L. Leifer (eds.), *Design thinking research. Understand – improve – apply* (pp. 111-128). Heidelberg: Springer.

European Quality Assurance Register for Higher Education (EQAR). (2024). *European Approach for Quality Assurance of Joint Programmes* (October 2014, approved by EHEA ministers in May 2015). Retrieved from https://www.eqar.eu/assets/uploads/2018/04/02_European_Approach_QA_of_Joint_Programmes_v1_0.pdf

Stiftung Akkreditierungsrat. (2024). *Akkreditierung von Joint-Degree-Programmen nach dem European Approach durch den Akkreditierungsrat* (Stand 02.11.2023). Retrieved from https://www.akkreditierungsrat.de/sites/default/files/downloads/2023/2023_11_02_Anerkennung-nachEA.pdf

ANNEX I

- Sample Accreditation Documents
  - Self Evaluation Report (SER)
  - Cooperation Agreement
  - Module Handbook
  - Study and Examination Regulations
  - Academic Staff CVs
  - Internal Quality Handbook
  - Student Handbook
  - Sample Degree Certificate
  - Sample Diploma Supplement
  - Sample Evaluation Questionnaires

Legal Disclaimer

Project 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03

Digital4Security

Shaping Europe's cyber future

ADVANCED DIGITAL SKILLS

DIGITAL EUROPE PROGRAMME

Co-funded by the European Union

Self Evaluation Report

Project details: Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty (Digital4Security)

Project ID: 101123430

Call: DIGITAL-2022-SKILLS-03

Introduction

The Joint Master's Degree Programme in **Cybersecurity Management and Data Sovereignty** is designed to deliver an innovative, comprehensive, and sustainable training pathway for the next generation of cybersecurity professionals. Developed under the "DIGITAL4Security – European Masters Programme in Cybersecurity Management & Data Sovereignty" project, this program is spearheaded by the University Politehnica of Bucharest (UPB), led by Prof. Ciprian Dobre, in partnership with a consortium of 36 institutions, including 13 academic partners and 23 associate partners. Funded by the European Union under the "DIGITAL-2022-SKILLS-03 - Advanced Digital Skills" initiative (project ID 101123430), the program unites top cybersecurity academic expertise from eight European countries and leverages industry insights from another eight nations. Through this collaborative effort, the program aims to set a new benchmark in advanced cybersecurity education, fostering expertise that addresses Europe's critical digital security challenges while ensuring graduates are equipped to lead in an evolving global cybersecurity landscape. By integrating both academic rigor and real-world industry insights, the program ensures that graduates are not only theoretically proficient, but also possess practical, employment-ready digital competencies, positioning them for long-term career success.

The Digital4Security consortium (sect. "Status") is united in its vision to establish a centralized hub for advanced cybersecurity education, which continually adapts to Europe's technological and cybersecurity landscape. An industry advisory board, with members from across Europe, has been established to ensure the program remains aligned with industry demands and technological advancements.

The Joint Master's Degree in Cybersecurity Management & Data Sovereignty is tailored for a wide range of learners in cybersecurity, from those entering technical fields to current professionals seeking to deepen their expertise. By delivering advanced cybersecurity knowledge and promoting a proactive, analytical mindset, the program empowers participants to excel in this critical field, driving innovation, resilience, and enhanced data protection in their organizations.

Delivered entirely online through synchronous and asynchronous methods, the program provides flexibility without requiring physical attendance. Each partner university contributes specialized expertise by serving as module owners within the curriculum.

Although mobility is primarily virtual in this program, learners have the option to attend physical networking events, hackathons, and collaborative activities hosted by partner institutions across Europe. This hybrid approach fosters international engagement while maintaining the accessibility and adaptability of an online format.

The program delivers a Master's Degree aligned with **Level 7** of the European Qualifications Framework (EQF), focusing on Advanced Digital Skills.

The quality assurance process for the DIGITAL4Security Master's programme is conducted in accordance with the **European Approach for Quality Assurance of Joint Programmes**, in collaboration with **VLUHR QA** as an internationally recognized quality assurance agency.

Terms and conditions of the joint programme are specified in the Cooperation Agreement (Annex 1).

This master's program has been developed by the **Digital4Security** consortium, including academic partners and industry partners. This pan-European approach ensures that both academic and industry knowledge is gathered comprehensively from across Europe, not being limited to the expertise, insights and experiences available in geographically more confined regions.

Standard 1. Eligibility

1.1 Status

The partners outlined in Table 1 share collective responsibility for the Joint Master's Degree in Cybersecurity Management and Data Sovereignty. They collaborate on research, module development, and curriculum delivery to address Europe's urgent need for cybersecurity expertise. United in their efforts, these partners are fully prepared to deliver the master's program currently submitted for accreditation.

Table 1: Academic Partners (Higher Education Institutes) Offering the Joint Degree Program

No.	Partner	Abbreviation	Country	Role
1	Universitatea Nationala de Stiinta si Technologies Politehnica Bucuresti	POLITEHNICA B.	Romania	Contributing
2	National College of Ireland	NCI	Ireland	Contributing
3	German University of Digital Science gGmbH	UDS	Germany	Degree-awarding
4	University of Rijeka	UNIRI	Croatia	Degree-awarding
5	Università degli Studi di Brescia	UNIBS	Italy	Contributing
6	Politecnico di Milano	POLIMI	Italy	Contributing
7	Universität Koblenz	UNI KO	Germany	Degree-awarding
8	CY Cergy Paris Université	CY	France	Contributing
9	Mykolo Romerio Universitetas	MRU	Lithuania	Contributing
10	Universidad Internacional de La Rioja	UNIR	Spain	Degree-awarding
11	Brno University of Technology	BUT	Czech Republic	Contributing
12	Munster Technological University	MTU	Ireland	Degree-awarding
13	Vytautas Magnus University	VMU	Lithuania	Contributing

The academic partners may serve in one of two roles: (i) as an awarding institution, officially listed on the degree document (Annex 7); or (ii) as a contributing partner institution, not listed on the degree document but included on the Diploma Supplement (Annex 8).

Table 2 provides further details on the academic partners, being accredited higher education institutions (HEIs) in their respective countries. Please note that the German University of Digital Science (UDS) is a new university, currently undergoing review by the German Akkreditierungsrat (GAR), with final approval expected by early December 2024, ahead of the program's accreditation timeline, which concludes by late December. The other institutions have already successfully completed their national accreditations.

Table 2: Additional Information on the Academic Partners

No.	Name	Point of Reference
1	University Politechnica of Bucharest	https://upb.ro/en/
2	National College of Ireland	https://www.ncirl.ie/
3	German University of Digital Science gGmbH	https://german-uds.de/
4	University of Rijeka	https://uniri.hr/en/home/
5	Università degli Studi di Brescia	https://www.unibs.it/en
6	Politecnico di Milano	https://www.polimi.it/
7	Universität Koblenz	https://www.uni-koblenz.de/en
8	CY Cergy Paris Université	https://www.cyu.fr/en
9	Mykolo Romerio Universitetas	https://www.mruni.eu/en/
10	Universidad Internacional de La Rioja	https://www.unir.net/
11	Brno University of Technology	https://www.vut.cz/en/
12	Munster Technological University	https://www.mtu.ie/
13	Vytautas Magnus University	https://www.vdu.lt/en/

1.2 Joint Design and Delivery

The joint program is collaboratively offered by the academic partners listed in the “Status” section, involving all participating institutions in both the design and delivery phases. Additional details on the collaborative process for design and delivery are provided in the “Curriculum” section.

1.2.1 Associate Partners

Partners other than Higher Education Institutes (HEIs) from the Digital4Security consortium do not participate directly in the accreditation process, as responsibility for the Master’s program rests solely with the HEIs. However, robust academia-industry collaboration remains a cornerstone of this program, warranting recognition of the partners listed in Table 3, who play a key role in shaping the program in several ways. They provided essential input during a comprehensive needs analysis, identifying specific cybersecurity challenges – particularly for small and medium-sized enterprises (SMEs) – that directly influenced the curriculum design. Furthermore, educational partners support the professional layout of module content (e.g., Profil Klett), the development of the online learning platform (Matrix), and the co-design of teaching materials in collaboration with academic partners (e.g., Cefriel, Ataya). Furthermore, industry partners offer internships, serve as expert mentors, and may also participate as panel members alongside academic faculty to provide feedback during practice-based capstone projects of the students.

This strong collaboration between academia and industry allows the consortium to align more closely with practical, real-world needs, offering students valuable hands-on experience. It stands in contrast to many traditional university programs that focus primarily on theoretical knowledge.

Table 3: Associate Partners

No.	Abbreviation	Associated Partner	Country
14	DTSL	DIGITAL TECHNOLOGY SKILLS LIMITED	Ireland
15	IT@CORK	IT@CORK ASSOCIATION LIMITED LBG	Ireland
16	SKILLNET	SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	Ireland
17	ADECCO TRAIN-ING	ADECCO FORMAZIONE SRL	Italy
18	ADECCO GROUP	ADECCO ITALIA HOLDING DI PARTECIPAZIONE E SERVIZI SPA	Italy
19	Adecco Italia	ADECCO ITALIA SPA	Italy
20	CEFRIEL	CEFRIEL SOCIETA CONSORTILE A RESPONSABILITA LIMITATA SOCIETA BENEFIT	Italy
21	Ataya	ATAYA & PARTNERS	Belgium
22	Cyber Ranges	CYBER RANGES LTD	Cyprus
23	FHG	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGE-WANDTEN FORSCHUNG EV	Germany
24	NASK	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	Poland
25	CMIP	POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPO-LAND SP. Z O. O.	Poland
26	SA	SCHUMAN ASSOCIATES SCRL	Belgium
27	Contrader	CONTRADER SRL	Italy
28	indiepics	INDEPENDENT PICTURES LIMITED	Ireland
29	MATRIX	MATRIX INTERNET APPLICATIONS LIMITED	Ireland
30	PROFIL KLETT	PROFIL KLETT D.O.O.	Croatia
31	ServiceNow	SERVICENOW IRELAND LIMITED	Ireland
32	DIGITAL SME	EUROPEAN DIGITAL SME ALLIANCE	Belgium
33	DIGITALEUROPE	DIGITALEUROPE AISBL*	Belgium
34	TERAWE	TERAWE TECHNOLOGIES LIMITED	Ireland
35	BANCO SANTAN-DER /Santander	BANCO SANTANDER SA	Spain
36	RED OPEN S.R.L.	RED OPEN S.R.L.	Italy

1.2.2 National Regulations

The Joint Degree Program is offered by a European consortium of Higher Education Institutions (HEIs) across eight European countries. In addition to pursuing European-level accreditation, each degree-awarding partner must secure accreditation within their own national system.

While national accreditation standards generally align with the European Approach, variations arise, especially concerning the recognition of online versus face-to-face education. The European Approach allows for fully online master's programs, yet certain countries maintain specific requirements, including stipulations for on-site components.

Further information on national higher education systems and regulatory frameworks is included in the Diploma Supplement (Annex 8).

Countries that Fully Accept Online Education:

Several European countries fully support online education, without imposing on-site requirements. These include Spain (ANECA), Germany (GAR), Croatia (ASHE), and Ireland (QQI).

Countries with Conditional or On-Site Requirements:

By contrast, some countries permit online education but impose additional requirements. Lithuania (SKVC) mandates that a small portion of master's programs include on-site learning while remaining largely flexible regarding online formats. Romania (ARACIS) traditionally does not permit fully online programs, but encourages blended learning with digital technologies, requiring at least 60 ECTS per year. Although processes in Romania are evolving, and there is openness to facilitate the European Approach, ARACIS requires that other nations involved in the joint degree follow the European standards and guidelines of quality assurance, as reviewed by the European Quality Assurance Register (EQAR). This is not yet the case in the Czech Republic, which endorses relatively independent approaches. Italy (ANVUR) currently has an evolving legal framework that traditionally requires on-site components, but is transitioning to accommodate online formats. Italy has also introduced a "Protocol for new distance learning degree programmes for the academic year 2024-2025," specifying additional requirements such as a Service Charter for student support, evaluation of physical and digital infrastructures, financial sustainability for online teaching, and thorough documentation of the program's technological architecture. Czechia (NAB) is currently unable to accredit international online programs.

Program Format

To comply with the Grant Agreement of the Digital4Security consortium and the varying national regulations, the master's program will be offered fully online. HEIs in countries unable to accredit the program nationally will participate as contributing partners, while those from countries permitting fully online education will serve as degree-awarding institutions.

1.2.3 Delivery Modalities and Student Mobility

The Joint Degree Program will be delivered **fully online** using **Moodle**,[1] a widely adopted learning management system (LMS) designed to facilitate interactive and collaborative learning. Moodle offers a variety of tools, including discussion forums, quizzes, multimedia content, and assignments, enabling students to engage with course materials at their own pace. The platform promotes collaboration through group projects, peer review activities, and real-time communication.

To ensure effective utilization of Moodle's features, all teaching partners have undergone training and will continue to receive ongoing support. Dedicated assistance is also available for students facing any issues, with support provided by both trained faculty members and industry partners specializing in the platform's functionalities. This comprehensive approach ensures a seamless learning experience for all participants.

As the program is delivered fully online, students are not required to attend classes in person at any partner institution. Instead, mobility will be primarily virtual, with students enrolling in modules taught by faculty from various institutional partners across Europe.

Beyond regular coursework, students will have the opportunity to engage in a range of **optional in-person events**, including networking sessions, hackathons, mentoring, and industry field trips. For those who prefer not to travel, remote participation will be available, ensuring accessibility for all learners. These events, hosted by partner institutions across different countries, will offer learners opportunities for meaningful interaction and optional physical mobility as part of the program's broader schedule.

1.3 Cooperation Agreement

The **DIGITAL4Security** programme is governed by a **Cooperation Agreement** defining the terms of the joint programme (Annex 1). This includes the degree title (Joint Master's Degree in Cybersecurity Management and Data Sovereignty), coordination and management responsibilities (covering financial management, cost-sharing, and revenue allocation), admissions and selection processes for students, mobility of students and faculty, as well as examination regulations, credit recognition, and degree awarding procedures across the consortium.

Standard 2. Learning Outcomes

The consortium has designed the Joint Degree Program through a multi-phase, comprehensive development process, and continues to refine it every step along the way.

The approach began with a rigorous market needs analysis to pinpoint existing and emerging cybersecurity skills crucial for companies, SMEs, and startups. Employing a mix of desk research, surveys, and interviews facilitated by industry partners, the consortium identified the necessary skill sets and formulated relevant Occupational Profiles based on the European Cybersecurity Skills Framework (ECSF). The consortium reviewed the collected data and established overarching learning goals for students completing the program (Table 4).

[1] www.moodle.com

Table 4: Overarching Learning Goals across the Joint Degree Program

No.	Goal
PO1	Critically assess and evaluate cybersecurity principles, practices, and technologies relevant to modern enterprises.
PO2	Strategically apply cybersecurity knowledge and utilise practical skills and technologies for long-term success in cybersecurity leadership roles across diverse industries, government agencies, and institutional settings.
PO3	Identify knowledge gaps and undertake self-learning to acquire new knowledge to support professional development and the ability to adapt to evolving threats, technologies, and regulatory environments.
PO4	Exhibit and apply leadership skills necessary for effectively managing cybersecurity initiatives within organisations, including education and training, strategic planning, and resource allocation.
PO5	Critically evaluate and analyse cyber threats in order to implement effective security operations, and to enable the proactive identification, assessment, and mitigation of cyber threats.
PO6	Effectively apply analytical and strategic thinking in order to make decisions to address security requirements.
PO7	Communicate effectively across a range of complex and advanced cybersecurity concepts to provide leadership within an organisation and facilitate effective collaboration and teamwork.
PO8	Critically assess cybersecurity legal, information governance, and regulatory frameworks and practices to ensure effective oversight, auditing, risk mitigation, accountability, compliance, and strategic alignment with organisational objectives.

These overarching learning goals are further enhanced by module-specific objectives, as explained in section “Curriculum”. Additionally, all modules within the program are carefully assessed and designed to align with the program’s learning goals, ensuring that they collectively contribute to a comprehensive educational experience. This alignment guarantees that students acquire the necessary skills and knowledge to excel in the field of cybersecurity management and data sovereignty, ultimately preparing them to meet the challenges of an evolving digital landscape.

Both for the program’s overarching learning goals and module-specific goals, learning outcomes are designed to be brief and concise, following Bloom’s taxonomy for level-appropriate assessment. They serve to clearly convey measurable objectives aligned with teaching content, ensuring transparency for students and educators regarding program expectations and evaluation criteria, thereby enhancing accountability.

2.1 Level [ESG 1.2]

The program implements a Master’s Degree corresponding to **Level 7** in the Framework for Qualifications in the European Higher Education Area **(QF-EHEA)**.

To ensure compliance, the learning goals and assessment methods for all modules undergo thorough and continuous review. This iterative process involves module developers creating content that is subsequently reviewed by experts from all participating higher education institutions (HEIs). Project management provides guidance to help developers formulate specific and measurable learning goals that emphasize higher-order skills in alignment with Level 7 standards, while also contributing to the program's overarching objectives. If any issues arise, the consortium has established a structured assessment approach to evaluate and enhance the alignment of learning outcomes with Level 7 standards (see Annex 9, Sample Questionnaire on Learning Outcome Assessment).

2.2 Disciplinary Field

The **DIGITAL4Security** project addresses the urgent need for cybersecurity expertise within European Small and Medium Enterprises (SMEs) and other organizations, aiming to protect industries from cyber-attacks and safeguard economic prosperity. Main program objectives include:

- **Upskilling and Reskilling**: Enhance the skills of graduates, professionals, and business leaders to strengthen cybersecurity infrastructure.
- **Bridging the Skills Gap**: Train students across various sectors, with a focus on individuals involved in smart technologies and high-value information management.
- **Flexible Learning Paths**: Offer tailored educational experiences that combine technical and managerial content to meet diverse industry needs.
- **Industry Collaboration**: Ensure a relevant adherence to market demands by a continuous and close relationship with European companies and SMEs in the programme's design and delivery.
- **Long-Term Competitiveness**: Contribute to Europe's economic growth by aligning with the European Cybersecurity Skills Framework (ECSF) and the goals of the DIGITAL Europe Programme.
- **Online-First Flexibility**: Maximize online content to provide flexible, inclusive access to cutting-edge cybersecurity education, regardless of location or personal circumstances.
- **Pan-European Expertise**: Utilize online collaboration to give students access to top specialists from leading institutions across Europe, delivering a more diverse and cutting-edge learning experience than local universities can offer alone.

The program's content is outlined in the curriculum description (sect. "Study Programme") and the Module Handbook (Annex 2), comprising 23 modules. Each module features intended learning outcomes that adhere to the Knowledge, Skills, and Competencies (KSC) framework:

- **Knowledge**: The theoretical understanding of a subject, encompassing facts, concepts, principles, and theories.
- **Skills**: The practical abilities necessary to perform specific tasks, developed through practice and experience.
- **Competencies**: The capacities that enable individuals to effectively perform in real-world situations, jobs and roles.

Detailed learning outcomes for each module can be found in the Module Handbook (Annex 2).

2.3 Achievement [ESG 1.2]

The Joint Degree Program is structured to encompass a total of 23 modules, balancing both mandatory and elective options to accommodate individual learning paths (typically, ENISA roles). Out of these 23 modules, 9 are mandatory, ensuring that all students acquire foundational knowledge and essential skills across core areas of cybersecurity. The remaining 14 are elective modules, providing flexibility for students to specialize in areas aligned with distinct occupational profiles. This modular approach supports learners in tailoring their educational experience to meet specific career goals while addressing emerging cybersecurity challenges across industries. The Master's Degree corresponds to a **total of 120 ECTS**.

The Cybersecurity Master's program demonstrates the achievement of its intended learning outcomes through a comprehensive strategy that integrates rigorous assessment methods, continuous feedback, and alignment with industry requirements. Each of the 23 modules outlines specific learning outcomes within the Knowledge, Skills, and Competencies (KSC) framework, enabling targeted assessments such as exams, projects, and practical exercises that effectively measure student progress. Regular feedback mechanisms ensure that students receive constructive insights into their performance, facilitating their growth and understanding of the subject matter. Furthermore, the program clearly maps each module's contribution to the overarching eight learning outcomes (see table 6 in the "Curriculum" section), ensuring transparency and a coordinated approach to achieving the educational goals. Engaging external evaluators and industry experts in the review process further validates the program's effectiveness in equipping students with the necessary skills for real-world scenarios. This industry consultation has been integral to curriculum design, and the consortium is committed to continuous quality management and improvement. Annex 9 includes sample questionnaires for industry experts to evaluate the program's relevance and quality in achieving the overarching goal of equipping students for cybersecurity roles, assessing each module individually. Additionally, student feedback (see Student Surveys in Annex 9) and analyses of performance across modules (Internal Quality Handbook, Annex 5) help gauge each module's effectiveness, ensuring participants meet the intended learning outcomes.

2.4 Regulated Professions

To ensure flexibility in terms of educational pathways, meeting diverse learners and industry needs, the curriculum has been designed in such a way as to equip students with the necessary skills for various ENISA profiles. ENISA (the European Union Agency for Cybersecurity) outlines specific competencies and skills relevant to different job roles in the cybersecurity field.

Based on the market analysis conducted in collaboration with industry partners, several job profiles have been identified, and corresponding curricula have been developed to ensure professional preparation. A final poll among all HEIs confirmed the inclusion of eight profiles in the Master's programme. This enables students to specialize in areas such as:

1. **Chief Information Security Officer (CISO)** - Focused on strategic leadership and management of an organization's cybersecurity approach (Fig. 1).
2. **Cyber Legal, Policy, and Compliance Officer** - Concentrating on the legal and regulatory aspects of cybersecurity, ensuring compliance with relevant laws and policies (Fig. 2).
3. **Cybersecurity Risk Manager** - Dedicated to identifying, assessing, and mitigating risks to information security (Fig. 3).

4. **Cyber Threat Intelligence Specialist** - Specializing in gathering and analyzing threat intelligence to inform defensive strategies (Fig. 4).
5. **Cybersecurity Educator** - Aiming to teach and promote cybersecurity awareness and best practices within organizations (Fig. 5).
6. **Cybersecurity Auditor** - Focused on evaluating and improving an organization's cybersecurity policies, practices, and controls (Fig. 6).
7. **Digital Forensics Investigator** - Specializing in the recovery and investigation of material found in digital devices, particularly relating to cyber crimes (Fig. 7).
8. **Incident Responder** - Concentrating on managing and responding to cybersecurity incidents to minimize damage and recover operations effectively (Fig. 8).

This targeted approach allows students to gain in-depth knowledge and skills tailored to their career aspirations in the rapidly evolving field of cybersecurity.

Fig. 1: A 120 ECTS Master's Program Preparing for the Role of *Chief Information Security Officer (CISO)* - Possible Pathway in a 2-Year Full Time Program

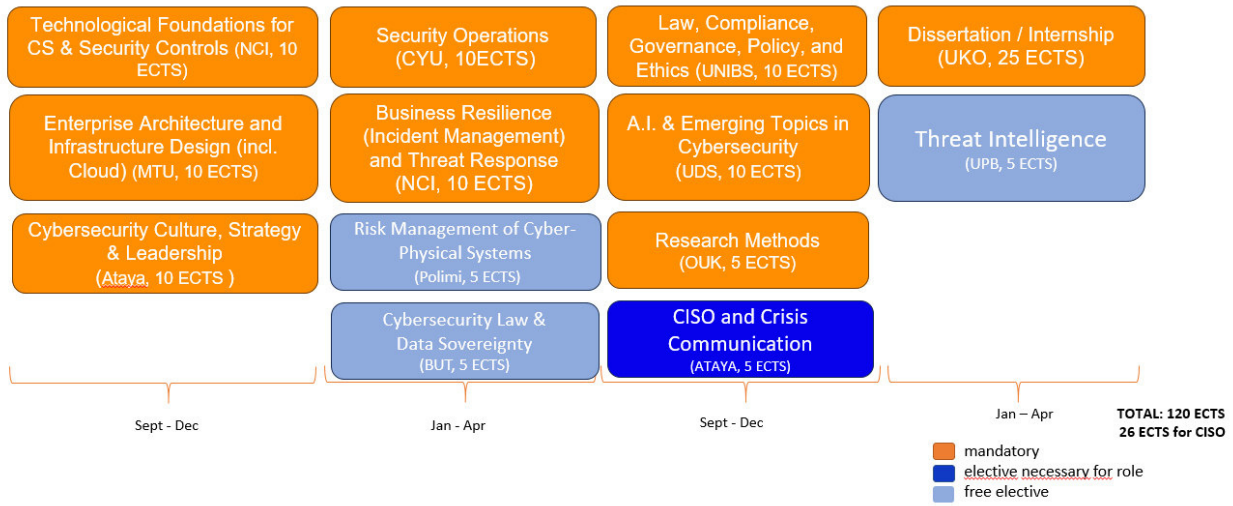


Fig. 2: A 120 ECTS Master's Program Preparing for the Role of *Cyber Legal, Policy, and Compliance Officer* - Possible Pathway in a 2-Year Full Time Program

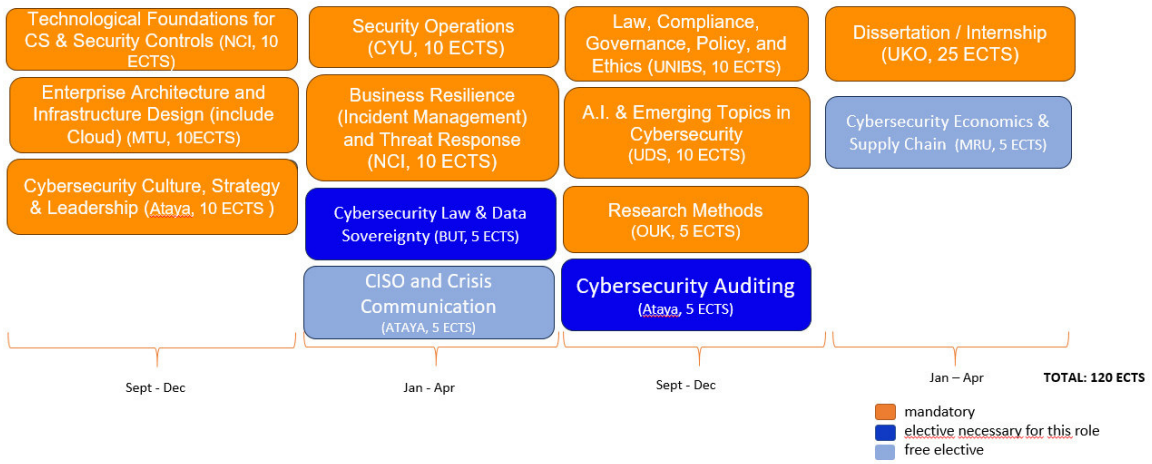


Fig. 3: A 120 ECTS Master's Program Preparing for the Role of *Cybersecurity Risk Manager* - Possible Pathway in a 2-Year Full Time Program

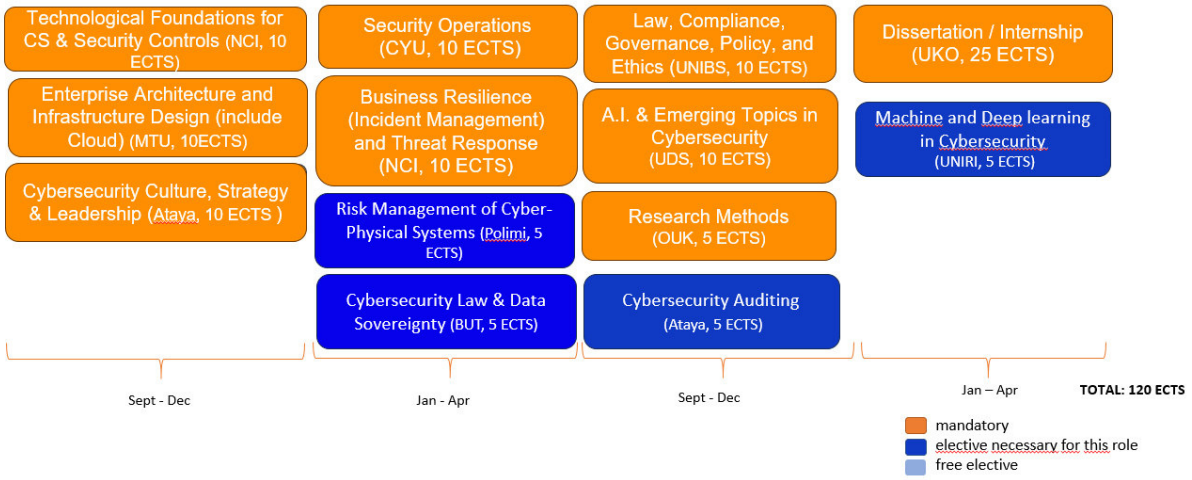


Fig. 4: A 120 ECTS Master's Program Preparing for the Role of *Cyber Threat Intelligence Specialist* - Possible Pathway in a 2-Year Full Time Program

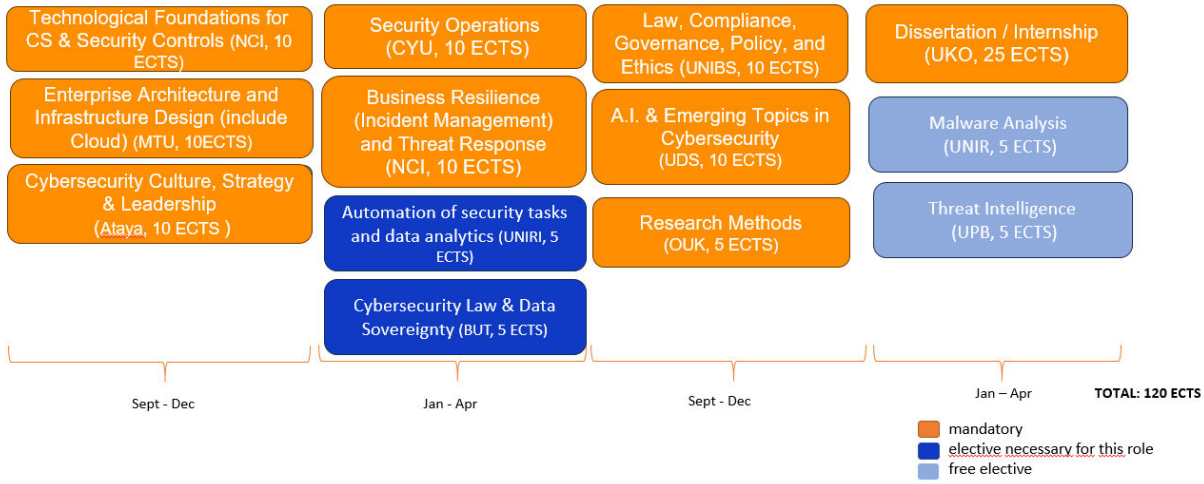


Fig. 5: A 120 ECTS Master's Program Preparing for the Role of *Cybersecurity Educator* - Possible Pathway in a 2-Year Full Time Program

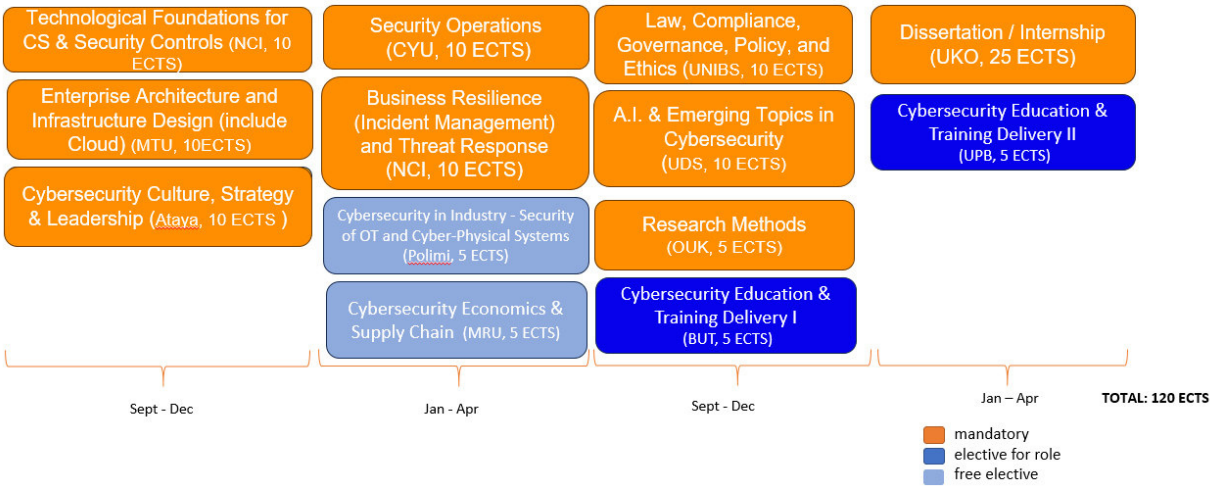


Fig.6: A 120 ECTS Master's Program Preparing for the Role of *Cybersecurity Auditor* - Possible Pathway in a 2-Year Full Time Program

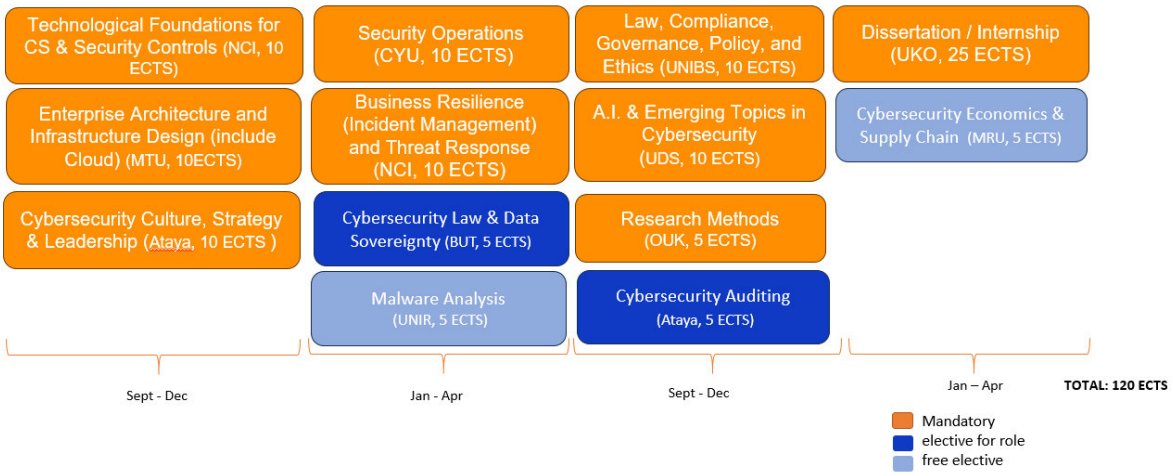


Fig. 7: A 120 ECTS Master's Program Preparing for the Role of *Digital Forensics Investigator* - Possible Pathway in a 2-Year Full Time Program

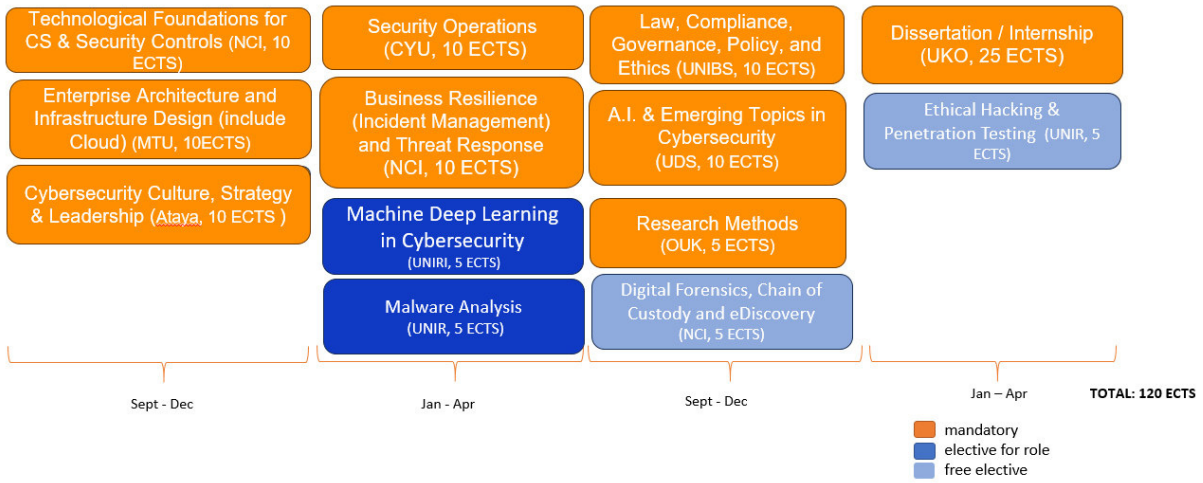
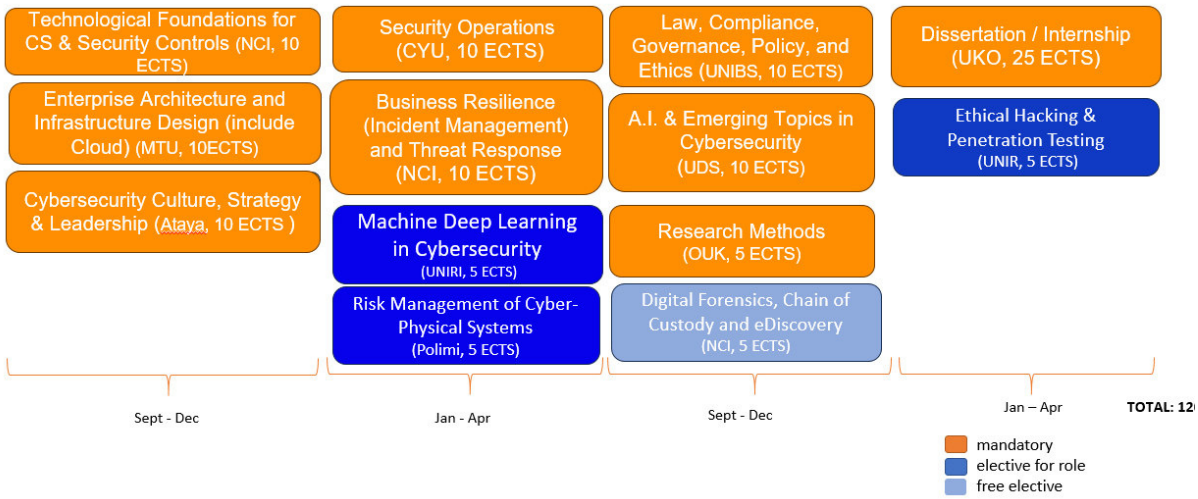


Fig. 8: A 120 ECTS Master's Program Preparing for the Role of *Incident Responder* - Possible Pathway in a 2-Year Full Time Program



Notably, the roles listed above, are **not classified as EU-regulated professions**. While they are crucial within the cybersecurity field, they do not fall under formal regulation by the EU, meaning there are no specific legal requirements or regulatory bodies that govern who can perform these jobs.

However, the DIGITAL4Security program aligns closely with the European Cybersecurity Skills Framework. It ensures adherence to internationally recognized standards and certifications. To achieve this alignment, the program actively collaborates with industry experts and advisory boards comprised of

professionals who hold certifications such as CISSP, CISM, and CTIA. This collaboration informs the curriculum design, ensuring that course content reflects the competencies required for these credentials. Furthermore, practical training modules are integrated into the program to prepare students for the certification examination processes associated with these qualifications.

Additionally, the program incorporates key regulatory frameworks, including the European Union General Data Protection Regulation (GDPR) and the European Cybersecurity Skills Framework (ECSF). This is achieved through dedicated coursework focused on data protection, compliance, and risk management practices, which are integral to maintaining regulatory standards in cybersecurity. By embedding these frameworks into the curriculum, students gain a comprehensive understanding of the legal and ethical considerations relevant to cybersecurity roles in Europe.

While the above profiles are not EU-regulated, the master's program will integrate **industry certifications**, leveraging strategic partnerships with key IT sector leaders. The program will offer industry certifications through Advanced Professional Microsoft Certificates and role-based certification programs. Students will have access to the necessary infrastructure for certification, including localized testing centers and online certification options.

Certifications will be embedded into the curriculum at key milestones to complement academic learning. Students will participate in preparatory training sessions led by industry experts, followed by certification exams in areas such as Advanced Professional Microsoft Certificates, Security, Compliance, and Identity, or specialized cybersecurity tracks. The exams will be proctored either in-person at designated centers or remotely, ensuring flexibility for full-time and part-time students. This certification process will be rolled out in three stages:

1. **Preparation**: Academic partners will provide study materials, tutorials, and mock exams to prepare students for industry certification tests.
2. **Examination**: Exams will be delivered through both physical and virtual testing environments, ensuring accessibility across the partner countries.
3. **Certification**: Upon passing, students will receive industry-recognized credentials alongside their academic degree, validating their skills for the job market.

Standard 3. Study Programme [ESG 1.2]

3.1 Curriculum

Our master's program includes both part-time and full-time study options, integrating academic and industry content to fast-track students into high-demand cybersecurity roles, such as Cybersecurity Risk Manager or Chief Information Security Officer (CISO) (see sect. "Regulated Professions"). To achieve these outcomes, 23 modules were designed, each led by one or two HEIS (Table 5).

Table 5: The Joint Degree Program Includes 23 Modules Conveying Distinct Cybersecurity Skills

No.	SUBJECT	ECTS	MAND/ELECT	PARTNER
1	AI & Emerging Topics in Cybersecurity	10	Mandatory	UDS
2	Business Resilience, Incident Management, and Threat Response	10	Mandatory	NCI
3	Cybersecurity Culture, Strategy & Leadership	5	Mandatory	VMU
4	Dissertation / Internship	25	Mandatory	UNI KO
5	Enterprise Architecture, Infrastructure Design and Cloud Computing	10	Mandatory	MTU
6	Law, Compliance, Governance, Policy, and Ethics	10	Mandatory	UNIBS
7	Research Methods	5	Mandatory	UNI KO
8	Security Operations	10	Mandatory	CY CERGY
9	Technological Foundations for CS & Security Controls	10	Mandatory	UPB
10	Automation of Security Tasks and data analytics	5	Elective	UNIRI
11	CISO and Crisis Communication	5	Elective	VMU
12	Risk Management of Cyberphysical Systems	5	Elective	POLIMI/ CEFRIEL
13	Cybersecurity Auditing	5	Elective	VMU
14	Cybersecurity Economics & Supply Chain	5	Elective	MRU
15	Cybersecurity Education & Training Delivery I	5	Elective	BUT
16	Cybersecurity Education & Training Delivery II	5	Elective	UPB
17	Cybersecurity in Industry - Security of OT and Cyber-Physical Systems	5	Elective	POLIMI
18	Cybersecurity Law & Data Sovereignty	5	Elective	BUT
19	Machine and Deep Learning in Cybersecurity	5	Elective	UNIRI
20	Digital Forensics, Chain of Custody and eDiscovery	5	Elective	NCI
21	Ethical Hacking & Penetration Testing	5	Elective	UNIR
22	Malware Analysis	5	Elective	UNIR
23	Threat Intelligence	5	Elective	UPB

The development of the modules has been an iterative process, incorporating quality assurance through extensive peer review. Initially, each module's foundational content was outlined by its owners, specifying **teaching methods** (such as lectures versus lab work), defining the **workload** (including contact vs. self-study hours), and allocating credit points. Prerequisites were identified alongside in-

tended learning outcomes encompassing **knowledge**, **skills**, and **competencies**. The content was organized weekly, incorporating varied **assessment formats** for grading and establishing clear passing criteria, supplemented by a reading list.

Once submitted, each module description underwent a comprehensive review by the entire consortium of cybersecurity experts, ensuring state-of-the-art content and consistent organization, for instance regarding the allocation of credit points relative to workload.

Only after receiving endorsement from the consortium, the modules became ready for implementation and delivery by the designated expert instructors.

The Module Handbook (Annex 2) provides detailed information on each of the programme's modules. The Cooperation Agreement defines the organizational bodies and their complementary roles in managing quality in teaching and examination. The Internal Quality Handbook (Annex 5) and the Sample Evaluation Questionnaires (Annex 9) outline the strategies and tools used to assess the effectiveness of the current curriculum, facilitating continuous improvements.

All modules are systematically designed to contribute to the overarching eight learning outcomes (see Table 6).

Table 6: Overview of Each Module's Contribution to the Program's Overarching Learning Goals.

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
A.I. & Emerging Topics in CyberSecurity	X	X	X		X	X		X
Business Resilience, Threat Response, and Incident Management	X	X	X	X	X	X	X	X
Cybersecurity Culture, Strategy & Leadership	X	X	X	X	X	X		X
Dissertation	X	X	X			X	X	
Internship			X	X		X	X	
Enterprise Architecture & Infrastructure Design	X	X			X	X		
Law, Compliance, Governance, Policy, and Ethics	X	X		X		X		X
Research Methods	X	X	X		X	X	X	
Security Operations	X	X			X	X		
Technological Foundations in Computer Science and Security Controls	X	X			X	X		
Automation of Security Tasks and Data Analytics	X	X			X	X		X
CISO and Crisis Communication	X	X		X	X	X	X	X
Risk Management of Cyber-Physical Systems	X	X			X	X		
Cybersecurity Auditing	X	X		X		X	X	X

Cybersecurity Economics & Supply Chain	X	X	X	X	X	X		X
Cybersecurity Education and Training Delivery I	X	X		X		X	X	
Cybersecurity Education and Training Delivery II	X	X		X	X	X	X	
Cybersecurity in Industry – Security of OT and Cyber-Physical Systems	X	X			X	X	X	X
Cybersecurity Law & Data Sovereignty (BUT)	X		X	X		X		X
Machine and Deep Learning in Cybersecurity	X	X			X	X		
Digital Forensics, Chain of Custody and eDiscovery	X	X			X	X	X	X
Ethical Hacking & Penetration Testing	X	X			X	X		
Malware Analysis	X	X			X	X		

Alongside the overall program learning outcomes, each module is aligned with specific learning aims. For example, in the "Business Resilience, Threat Response, and Incident Management" module, distinct learning goals have been established, as outlined in table 7. This structured approach ensures that each module not only aligns with the broader objectives of the program, but also offers specialized abilities pertinent to specific areas of cybersecurity.

Table 7: Sample Module Learning Objectives Specified for the Module "Business Resilience, Threat Response, and Incident Management"

No.	Goal
MLO1	Evaluate incident response plans, their effectiveness and their alignment to industry leading standards and appropriate incident response principles and methodologies.
MLO2	Critically appraise response activities for incident management from initial compromise to recovery and make recommendations for improvement.
MLO3	Contrast methods to assess the maturity of an organisation's incident response capabilities.
MLO4	Evaluate mechanisms to leverage blue team and the red team capabilities during an incident and appraise appropriateness and prioritisation for specific incident response use cases.

3.2 Credits

The program is designed with a flexible curriculum structure that accommodates both part-time and full-time online Master's students.

The **full-time program comprises 120 ECTS**, to be completed over **two years** across four semesters. The **part-time program also consists of 120 ECTS** but is spread over **three years**, completed across six semesters.

Once European accreditation is obtained, the Digital4Security consortium furthermore aims to offer the program modules as **micro-credentials** under national accreditation regulations, expanding the program's reach yet further and offering students even more flexible study options.

3.3 Workload

The program schedule is designed to distribute workload as evenly as possible across semesters by offering a variety of teaching and assessment formats. Before each academic semester begins, the Joint Programme Committee sets the timetable and class schedule. Assignment release and submission dates are also determined in advance to ensure a fair and balanced distribution of assessment workload for learners.

Each semester includes 12 weeks of teaching, followed by time allocated for final exams. In the full-time program, students can earn 30 ECTS per semester over four semesters, with a workload of approximately 750 hours per semester (1 ECTS = ~25 hours of student work). This workload includes both attendance-based learning and self-study of all compulsory elements, with detailed workload estimates available for each module.

The part-time program schedules 20 ECTS per semester, corresponding to around 500 hours of work. For students who may not be able to invest this amount of time per semester due to family or job responsibilities, micro-credentials offer yet more focused study options. As the program module typically correspond to 5 or 10 ECTS, they offer targeted upskilling opportunities at workloads of about 125 or 250 hours per semester.

This flexible program structure accommodates various student groups: recent graduates seeking a full-time and intensive program; industry professionals pursuing part-time studies to enhance their skills alongside work; and students looking for focused upskilling through customizable micro-credentials.

As part of internal quality management, student feedback is collected after each semester, including questions on actual workload experienced per module (see Annex 9, student questionnaire). This feedback allows adjustments should any discrepancies be found towards the module's ECTS credits and expected workload. Additionally, student support services are available to assist learners in case they experience any challenges related to workload (see sect. "Student Support").

Standard 4. Admission and Recognition [ESG 1.4]

4.1 Admission

The admissions process is regulated in the Cooperation Agreement (Annex 1). It is designed to be transparent and equitable, overseen by the **Joint Admissions Board**, which comprises representatives from all academic partners. This Board is responsible for setting high standards, managing the selection process, and ensuring a fair and consistent evaluation of all applicants.

To facilitate this, application deadlines are clearly outlined on the official program webpage www.digital4security.eu. Prospective students are encouraged to regularly check this site for updates and specific dates related to each admission cycle. Applications must be submitted through the designated

online application portal, accessible via the program's webpage. Detailed instructions will be provided to guide applicants through the application process, ensuring clarity and ease of use.

Several key bodies collaborate to support the admissions process. The **Joint Admissions Board** oversees the overall process, while the **Master's Board of Directors** provides strategic guidance and final approval of admissions decisions. Additionally, the **Secretariat** manages administrative tasks, ensuring smooth communication among all parties involved, and collecting tuition fees.

To qualify for admission, applicants must hold at least an **EQF level 6 qualification**, such as a bachelor's degree in a relevant field like Computer Science, Information Technology, Cybersecurity, or equivalent disciplines. Degrees in related areas, such as Engineering, Mathematics, or Data Science, may also be considered; in such cases, the selection committee evaluates the curriculum content for relevance.

The program is inclusive and also considers applicants without formal qualifications, who can demonstrate relevant skills and knowledge through professional experience, portfolios, or certifications like CompTIA Security+, CCNA, or Advanced Professional Microsoft Certificates. These applicants can submit evidence, such as work samples and detailed CVs, which will be evaluated against established criteria by the **Joint Admissions Board**.

In addition, applicants must demonstrate English proficiency through recognized tests, including a minimum IELTS score of 6.0, a TOEFL (IBT) score of at least 100, or a CEF-level of B2. Furthermore, all applicants are required to have access to a reliable computer, internet connection, and necessary software to effectively participate in online learning and virtual activities.

The assessment process involves submitting an application form, academic transcripts, two letters of recommendation, and a personal statement that outlines the applicant's motivation and career goals. All materials are submitted online, and the **Joint Admissions Board** assesses applications based on academic merit and the potential for success. For applicants lacking formal qualifications, alternative pathways such as micro-credentials or preparatory courses may be recommended to help meet program standards, promoting inclusivity and continuous learning.

Shortlisted candidates may be invited for interviews to further assess their suitability for the program. The selection process is thorough, with multiple committee members independently reviewing each application to ensure a comprehensive and unbiased evaluation. This structured approach not only upholds the integrity of the admissions process, but also reinforces the program's commitment to attracting diverse and capable candidates.

Quality Assurance regularly assesses whether students possess the necessary prerequisite knowledge based on current regulations and makes adjustments as needed. For example, if students with minimal English proficiency are found to perform below average in terms of grades and completion rates, strategies like offering "English for Cybersecurity" courses or raising admission thresholds will be considered.

4.2. Recognition

Applicants lacking the minimum academic qualifications will have their entry assessed based on prior learning and work experience, as well as a demonstrated commitment to meeting academic standards. The assessment will include a written application and an interview, with recognition aligned to the

program's Recognition of Prior Learning (RPL) policy (cf. Cooperation Agreement, Annex 1). Applicants are required to submit a portfolio of evidence, including syllabi from completed courses.

The **Joint Admissions Board** will evaluate the applicants' numeracy skills based on the evidence provided, typically considering prior completion of modules with significant numerical content. If evidence of sufficient numeracy skills is lacking, applicants may be required to complete an assessment.

Non-standard applicants may possess extensive work and life experience that merits access to the program. The RPL policy serves as a guideline in these cases, emphasizing that "learning" encompasses both conceptual understanding and practical application of knowledge.

Applications for RPL consideration should be made through the centralized admissions platform. All applicants seeking RPL entry will be interviewed; they are required to submit a portfolio detailing their prior experiences in relation to potentially creditable learning outcomes. The portfolio will be assessed for validity, sufficiency, currency, and authenticity.

- **Validity:** Does the submitted evidence meet the necessary requirements or standards for admission?
- **Sufficiency:** Is the evidence adequate to demonstrate that the applicant meets the qualifications needed for entry?
- **Currency:** Is the evidence recent? We expect any relevant experience or qualifications to have been obtained within the last five years.
- **Authenticity:** Is the evidence genuinely showing the applicant's own work?

Assessors will consider whether the learning gained from experience aligns with the programme content, applying criteria such as the balance between theory and practice, the transferability of learning, and whether the applicant has achieved an appropriate academic level, specifically meeting EQF level 6 qualifications for admission.

This RPL policy aligns with the aims and principles of the Lisbon Recognition Convention and its and subsidiary documents by providing a transparent framework for recognizing prior learning and experience, allowing applicants without formal qualifications to demonstrate their competencies through comprehensive portfolio submissions. This policy emphasizes fairness and consistency in assessment, ensuring that applicants are evaluated based on clear criteria related to the validity, sufficiency, currency, and authenticity of their prior learning. Additionally, it supports flexibility in recognizing substantial differences in qualifications while adhering to national education frameworks, thereby fostering equitable access to higher education opportunities.

Standard 5. Learning, Teaching and Assessment [ESG 1.3]

5.1 Learning and Teaching

The Digital4Security program employs a progressive Teaching, Learning, and Assessment (TLA) strategy designed to actively engage learners with module content and showcase their understanding. This strategy integrates diverse instructional methods, including lectures, tutorials, problem-based learning

(PBL), inquiry-based learning, practical work, flipped classrooms, seminars, case studies, project work, and collaborative group activities, all recognized for their effectiveness in fostering deep learning.

Central to our approach is the belief that learners should be active participants in their educational journey. We strive to make content relevant to real-world applications, encouraging interaction among peers and faculty from partner institutions within a supportive learning environment. Practical tutorials expose students to industry-relevant technologies, enabling them to connect theoretical knowledge with practical skills.

Our commitment to excellence in teaching drives us to explore new strategies such as game-based learning and gamification, enhancing student engagement and motivation. Leveraging state-of-the-art technology, our synchronous online classes replicate the interactivity of traditional face-to-face settings, featuring live discussions, screen sharing, breakout rooms, and recorded sessions for flexible review.

The fully online program utilizes a centralized Learning Management System (Moodle) and virtual classroom technology to facilitate learning activities, providing a seamless experience for learners. Asynchronous tasks, such as audio/video presentations and practical exercises, complement synchronous live lectures and labs, allowing students to engage with materials both independently and collaboratively.

Further details on the Teaching and Learning approach are outlined in the Student Handbook (Annex 6). In essence, teaching and learning are understood as a collaborative process involving students, lecturers, and academic support staff, with students at the center.

Students can expect the programme teaching and support staff to:

- Treat all learners with dignity and respect
- Provide academic support and guidance
- Provide appropriate teaching and learning materials
- Provide a Module Descriptor for each Module studied
- Assess your learning in ways that are fair, consistent and valid
- Assure fair and consistent enforcement of all programme rules and procedures

In turn, Students are expected to:

- Treat all teaching and support staff and students with dignity and respect
- Take responsibility for their own learning
- Attend all classes, tutorials and other learning sessions
- Make proper use of all learning resources provided
- Attempt honestly all assessments set on their programme
- Abide by all the programme‘s rules, regulations, and procedures

Teaching attempts to create a relevant and meaningful context for learners to make practical connections to the knowledge and skills being acquired. This is primarily achieved through the broadly practical nature of tutorials across most modules which expose students to industry-based technologies, techniques and challenges through practical laboratory exercises.

Teaching styles and contexts are flexible and aim to motivate and engage learners. Assessments are recognised as learning opportunities, and are designed to match the level of study, and to prepare learners for progression.

The part-time programs are delivered entirely online through Directed E-Learning (DEL), which combines on-demand activities and live online classes using virtual classroom technology. Students will complete specific tasks independently at scheduled times on the program's Learning Management System (LMS). This approach helps avoid overcrowded schedules, especially for students with limited time, and allows the program team to keep track of student progress and engagement in the online courses.

For Full Time programmes, both lecture and practical labs/tutorials will be delivered fully online. Full Time learners will also be able to avail of DEL assets and resources.

Examples of asynchronous activities include audio and video presentations, podcasts, practical lab and project work, as well as asynchronous discussion activities. By contrast, examples of synchronous activities comprise live lectures, live labs, and group work in breakout rooms.

Students are required to upload their asynchronously produced work to the Learning Management System (LMS) on a weekly basis. The synchronous class sessions are designed to build on and enhance these asynchronous and self-paced materials on Moodle. This structure enables learners to engage with the content outside of class, allowing class sessions to concentrate on the practical facilitation and application of the covered materials.

Learners are given the tools and guidance to create and manage their own digital spaces where they can organise group work/study groups/support chats etc.

Due to the fully online delivery mode, the program team will ensure that:

- Learners are informed in advance about the technical requirements and prerequisite skills needed for effective course participation.
- Learners receive comprehensive support during the introductory phase, specifically focused on how to navigate and utilize the learning technologies associated with the program.
- Ongoing professional development and support are provided to the program staff to enhance their skills in designing, producing, and utilizing new technologies for teaching and learning.
- Robust technical support is readily available for all systems utilized by the program, including the Learning Management System (LMS) and Learner Portal.
- Program and module learning outcomes, along with associated assessments, are standardized across all delivery modes, unless specifically stated otherwise and approved.
- Lecturers are encouraged to employ effective pedagogical design in their planning and production of learning activities, achieved by mapping these activities to specific learning outcomes.

- Learners have access to archived instructional sequences for review and revision purposes, reinforcing their understanding of the material.
- Learner assignments are submitted electronically through the LMS, unless otherwise specified, streamlining the submission process.

Overall, the learning and teaching framework is designed to meet the needs of a diverse student body, respecting various life situations and cultural differences, while providing support for students with disabilities. This commitment is evident in both the program design and its stringent quality management processes. Each semester, all modules undergo a thorough review that gathers feedback from both students and lecturers regarding inclusivity and accessibility (Annex 9). If any issues are identified, lecturers can adjust their teaching methods, and the **Master's Board of Directors** can implement strategic improvements for the program. Additionally, mentorship and support services are available to students (sect. “Student Support”).

5.2 Assessment of Students

Assessments are thoughtfully designed as learning opportunities, ensuring they align with the program's academic standards. They undergo rigorous quality assurance processes to validate that learning objectives are appropriately met. Furthermore, we prioritize the professional development of all educators involved in the program, ensuring they are well-prepared to support students effectively.

Further information is provided in the Study Handbook (Annex 3). In essence, the assessment framework follows the principle of constructive alignment, ensuring a close relationship between intended learning outcomes, teaching formats, and assessment methods. Exams are designed to evaluate the extent to which students achieve these defined learning objectives. Each module is accompanied by a Module Descriptor, outlining the types of assessments, including possible alternatives. At the start of each module, learners are informed about the conditions for completion, such as coursework and exams. Assessments are marked based on transparent criteria, and grading rubrics are provided. Lecturers offer timely feedback, typically within two weeks of submission, and learners can request additional feedback meetings.

Assessment instruments are chosen based on five key principles:

1. **Student Responsibility:** Students must submit assessments to demonstrate their achievement of the program's learning outcomes.
2. **Standards Alignment:** Grades are awarded based on assessments that evaluate specific criteria, including knowledge, skills, and competencies.
3. **Support for Learning:** Effective assessment is integral to teaching and learning, aligning with intended learning outcomes.
4. **Regular Review:** The Joint Programme Committee, alongside the Quality Enhancement and Curriculum Development Committee, regularly reviews assessment methods to meet evolving requirements.
5. **Transparency:** Students are informed about the assessment processes and regulations, ensuring they understand the module and program learning outcomes.

All modules incorporate formative assessments through individual or group activities to gauge learning progress, with practical lab work completed weekly during mentoring and tutoring hours. Each module includes one or two additional assessments, which may consist of:

- **Open Book Examinations:** Allowing students to demonstrate understanding and research capabilities.
- **Peer Reviews:** Enabling critical analysis skills.
- **Individual and Team Projects:** Fostering practical and leadership skills.

Examinations and assessments adhere to the policies established by the **Master's Board of Directors**, with joint **Examination Regulations** agreed upon by all partner institutions. The **Examination Board** ensures compliance with these regulations.

Documentation detailing assessment rules is readily available to students, with the Modules Handbook specifying assessment types, their contribution to overall marks, and timing. Students may apply for repeat assessments if they fail a module; if they fail again, re-enrolment is required.

For more information on examinations and assessments, please refer to the Study and Examination Regulations (Annex 3), which will be made available to students on the program's website.

Standard 6. Student Support [ESG 1.6]

Regular support for students in the programme is provided by academic and support staff, with the Programme Coordinators holding primary responsibilities. Beyond this, a comprehensive range of additional services is offered to help students navigate various challenges they may encounter and to reach their full potential.

Information about these student support services can be accessed online through the student support services portal on the programme website. Students can submit requests for support services via this portal, with Programme Coordinators serving as the initial point of contact to process these requests.

The **Learning Development Support Service** is dedicated to empowering all students in becoming active and confident learners. This is achieved through initial engagement during the orientation phase and ongoing support in developing effective academic skills throughout the semesters. The service focuses on integrating innovative learning technologies for enhanced learning experiences, and feedback to promote metacognitive awareness. By helping learners reflect on their pathways, the service supports them in learning how to learn, and in developing effective personal learning strategies, which expand individual strengths and address potential weaknesses. Additionally, it accommodates diverse learning preferences, creating an inclusive environment that encourages all students to thrive.

The **Disability Support Service** aims to ensure that students with disabilities can reach their full potential by providing tailored support that addresses their specific needs. The program is committed to offering equal access to education and equal opportunities for students with disabilities, ensuring that they receive the necessary resources and accommodations to succeed academically. This initiative collaborates closely with the **Assistive Technology Support Service**, which focuses on removing educational barriers by leveraging technology. By offering customized technology solutions and personalized training, this service promotes independent learning and enhances the overall academic experience for each student.

The **Careers and Opportunities Support Service** is a key component of the Employability Strategy, aimed at enhancing the students' job readiness through a range of scheduled events. These activities include online, hybrid, and in-person formats. They serve to promote collaboration with industry partners from the Digital4Security consortium and the wider business community. Furthermore, the service equips students with vital career management and employability skills while offering extensive information on diverse career paths available to both current students and recent graduates.

The **Student Counselling and Wellness Service** offers a nurturing environment where students can openly discuss any challenges they face during their studies. Pursuing a Master's degree can be overwhelming, and students may encounter academic, career, or personal obstacles that affect their overall experience. The counselling service provides a confidential space for students to explore various concerns, including:

- Stress
- Anxiety
- Academic difficulties
- Relationship issues
- Depression
- Family problems
- Grief or bereavement
- Homesickness or loneliness
- Identity issues
- Physical assault or abuse
- Self-harm
- Eating disorders
- Addiction or substance abuse
- Confidence or self-esteem
- LGBTQ+ support
- Autism, ADHD, and neurodiversity support

Students can schedule appointments with the Student Counselling and Wellness Service by emailing the office, after which a counsellor will reach out to arrange an available time. Each counselling session lasts between 40 to 50 minutes, with the frequency and duration of sessions tailored to individual needs, typically occurring weekly or bi-weekly, and ranging from one to six sessions.

The **Library Service** is a vital resource for students, offering access to a diverse range of scholarly publications. In an era where information is abundant online, it is crucial for students to develop the skills to navigate both credible and less reliable sources. The programme's library services provide a comprehensive collection of high-quality online resources essential for successful academic study. Students can access the library catalogue online, searchable by author, title, or keywords. Core texts and articles specified in the reading list are readily available through the programme's library services.

To ensure effective service delivery, the Digital4Security consortium will allocate adequate resources, including funding for the development and maintenance of essential materials. Additionally, financial support will be directed towards enhancing training for staff to provide support, and for students to utilize resources effectively. This approach fosters a comprehensive learning environment that addresses diverse educational needs.

Standard 7. Resources [ESG 1.5 & 1.6]

7.1 Staff

The curriculum for the Joint Master's Degree Programme in Cybersecurity Management and Data Sovereignty has been collaboratively designed by faculty members from each partner institution, together with the broader Digital4Security consortium. This joint effort ensures that the programme is both comprehensive and rigorous. Each partner institution brings experienced teaching staff with in-depth knowledge across the range of topics covered in the programme, ensuring that all aspects of the curriculum are effectively addressed.

Faculty members across the partner institutions possess expertise in both the required subject matter areas and pedagogical skills. Their research activities and qualifications align with the programme's content and intended learning outcomes, enabling students to engage with current, relevant issues in the field. For further details on faculty qualifications and professional backgrounds, please refer to Annex 4, which includes CVs for all lecturers responsible for the modules listed in the Module Handbook (Annex 2). This documentation confirms the sufficiency and high qualifications of our faculty, underscoring their expertise, professional experience, and commitment to delivering high-quality training.

In the spirit of quality management and to ensure continuous improvement, learner feedback will be collected through course evaluation surveys (Annex 9) after each semester, covering all modules. The survey outcomes will be shared with lecturers, offering valuable insights to help refine pedagogical strategies and adapt teaching methods to better meet student needs and expectations. This feedback loop is essential for aligning instructional approaches with evolving learner requirements.

In addition, on an annual basis, the **Master's Board of Directors** will review whether the subject-specific and didactic qualifications of the faculty adequately contribute to the successful delivery of the programme.

Furthermore, a Train the Trainer programme will be implemented for teaching staff. This initiative provides training on the practical use of online tools, the Learning Management System (LMS), and pedagogical strategies for effective online course delivery.

7.2 Facilities

The fully online Master's programme in Cybersecurity Management and Data Sovereignty is supported by a centralized digital platform designed to comprehensively meet learning and administrative objectives through highly integrated, secure, and accessible tools. From initial inquiries to graduation, this platform creates a seamless journey for students, enabling access to all educational and administrative functions from a single point of entry at www.digital4security.eu.

To effectively offer and manage the program, the platform incorporates two vital components: a Customer Relationship Management (CRM) system and a Learning Management System (LMS).

The CRM plays a fundamental role in managing the entire student life cycle, from initial interactions and application processing to module registration, grading, and degree awarding. Full Fabric, a CRM known for its specialization in higher education, is under consideration to support these functions,

although other sector-specific CRM options are also being reviewed to ensure the most robust solution for personalized student interactions and centralized programme management.

Moodle has been selected as the LMS, providing a flexible, user-friendly platform that is well-suited for delivering a fully online, interactive program. It supports both asynchronous and synchronous learning (see sect. “Delivery Modalities and Student Mobility”) and offers a robust suite of tools for seamless interaction and collaboration. With its extensive range of plugins, integration capabilities, and advanced analytics, Moodle enables detailed tracking of student progress and engagement, allowing faculty to make informed adjustments that continuously enhance the learning experience.

Both the CRM and LMS are hosted on secure, scalable cloud infrastructure, featuring load-balancing capabilities, real-time monitoring, identity and access management, and robust data storage solutions. This setup ensures high performance, security, and resilience, allowing students and faculty to reliably access all resources and functionalities from anywhere.

Further enhancing the program, integrated lab services support hands-on learning in areas such as collaborative coding, private code repositories, and Continuous Integration/Continuous Deployment (CI/CD) workflows – key elements for developing practical skills alongside theoretical understanding. A more detailed overview of web resources can be found in the Student Handbook (Annex 6), specifically in the section on Resources.

Overall, the facilities required for implementing an online Master’s program are relatively affordable and widely accessible, primarily relying on existing internet infrastructure along with the necessary software and hardware. The departments of higher education institutions involved in program delivery are all specialized in cybersecurity and related IT domains, making such infrastructure part of their basic equipment. This moderate demand for facilities enables the program to offer a highly economical study option, allowing participants from across Europe to access state-of-the-art cybersecurity education in a cost-effective manner (cf. sect. “Conclusion”).

Participation in the online education program requires students to have personal computing equipment, specifically a PC or laptop, as well as reliable internet access with sufficient bandwidth. These technical requirements are outlined as part of the program’s admission criteria (sect. “Admission”).

Standard 8. Transparency and Documentation [ESG 1.8]

A full set of Module Descriptors is accessible to all learners and teaching staff, containing the following information:

- Module title
- Person(s) responsible for each module
- Teaching method(s)
- Credits and workload
- Intended learning outcomes
- Module content
- Admission and examination requirements
- Form(s) of exams and details explaining how the module mark is calculated
- Recommended literature
- Date of last amendment

- When applicable: The deadline for withdrawing from the course (the day before the first graded course assessment).

Module Descriptor information and documentation can be downloaded via links provided on the website.

Additionally, the following documents are available for download from the website:

- Student Handbook
- Exam & Study Regulations
- Fees Information

Diploma and Diploma Supplement

Students who have satisfied all requirements of the final assessment will be awarded the Joint Master's degree as per the Cooperation Agreement (Annex 1). Those who have not met all requirements within the program duration will be required to re-register and pay extension fees.

The degree awarded will be confirmed by the issuance of a Master's Diploma (Annex 7) and Diploma Supplement (Annex 8). The Diploma Supplement will adhere to the template developed by the European Commission, the Council of Europe, and UNESCO/CEPES and will be adapted to comply with any further specifications in national legislation where applicable. The Diploma Supplement will be provided in English. The Degree Certificate will be issued as a Joint Degree on behalf of the higher education institutions (HEIs) that are signatories to the Cooperation Agreement.

Marks for each completed module will be recorded on the Diploma Supplement. The overall final mark will be computed as a weighted average, taking into account the results of each module weighted by the module's ECTS contribution.

Relevant Rules

The Digital4Security consortium aims to make all information and documentation pertaining to the study program easily accessible. The main Digital4Security website serves as a centralized hub for program information, while each HEI partner's website will also provide details about the joint program and links to the central Digital4Security website. The following information will be readily available to students and prospective students:

- Program content and structure
- Admission requirements
- Fees information
- Application and selection procedures and deadlines
- Qualifications and degrees awarded
- Student experience and employment prospects

The Secretariat and Program Coordinators support all partner institutions in providing accurate and up-to-date information through their student advisory services and websites.

Prospective students are encouraged to attend online open day or open evening events, where they can discuss any questions related to the program with representatives from the **Master's Board of Directors**.

Prior to the start of the program's class sessions, students will receive essential information about the program and its tools through a series of online orientation activities. During these sessions, they will also have the opportunity to network with fellow students, including members of the alumni network.

Students will find all non-public documents and information relevant for their studies embedded in their LMS platform and in closed sections on the central programme website.

Standard 9. Quality Assurance [ESG 1.1 & part 1]

The management of the program will adhere to the quality assurance procedures established for the Joint Master's Degree in Advanced Digital Skills, as detailed in the Internal Quality Handbook (Annex 5), which has been collectively agreed upon by all partner higher education institutions (HEIs). These procedures include annual program monitoring and review, alongside assessment protocols. Sample questionnaires for gathering feedback from relevant parties such as students, lecturers and industry experts are included as Annex 9.

The quality assurance framework outlines the roles of the **Master's Board of Directors** and relevant committees, such as the Programme Coordinators and the Quality Enhancement and Curriculum Development Committee, illustrating their integration into the overall academic governance of the program. A well-orchestrated set of academic bodies and quality management mechanisms will monitor and enhance the program, incorporating feedback from learners, faculty, and industry experts. Key approaches are summarized in Table 7.

Table 7. Feedback Mechanisms from Academic Structures and Processes

Body/Mechanism	Contribution
Master's Board of Directors	Responsible for developing and monitoring the implementation of academic policies, particularly concerning quality assurance for programs and initiatives.
Class Representatives	Each cohort elects two representatives to consult with academic and support staff regarding program content, delivery, assessment, and areas of concern. Meetings occur at least once a semester, facilitated by the Programme Coordinators.
Learner Feedback Surveys	Conducted at the end of each semester to gather student perspectives on the program, including content, delivery modalities, tools, and social experiences.
Lecturer Feedback Surveys	Conducted at the end of each semester to gather lecturer perspectives on the program, highlighting best practices and areas for improvement.
Industry Expert Surveys	Conducted annually to gather insights from industry experts regarding the quality, relevance, comprehensiveness, and currency of each module and the program overall.
Joint Programme Committee	Central to the program's quality assurance system, this committee collaborates with the Master's Board of Directors and the Quality Enhancement and Curriculum Development Committee to develop and oversee the program, ensuring quality delivery and fair assessments.
Annual Programme Review Report	The Quality Enhancement and Curriculum Development Committee will monitor program performance annually, summarizing data and findings, and suggesting implications. This document is reviewed by the Master's

	Board of Directors to identify potential strategic adjustments and interventions.

The Annual Programme Review Report typically includes:

- **Approved changes to the curriculum** and its components, following established procedures.
- **Presentation and analysis of retention, progression, and completion statistics** for the last two semesters, compared to previous years.
- **A review of learner intakes.**
- **Summaries of learner statistics per module** with subsequent interpretations.
- **Summaries of feedback** from students, lecturers, and industry experts, along with interpretations.
- **Reflections on program performance,** including quality assessments and potential strategies for improvement.
- **Review of required materials and equipment** for students.

The Annual Programme Review Report will be publicly available, ensuring full transparency for students and other stakeholders.

Conclusion

The Joint Master's Degree Programme in Cybersecurity Management and Data Sovereignty embodies a forward-thinking approach to cybersecurity education, driven by a vision to equip European SMEs and businesses with the essential skills to navigate the complexities of cyber threats. As we stand ready for accreditation, this program is poised to fulfill its mission of providing market-driven, industry-aligned education that evolves in tandem with emerging cybersecurity challenges.

Strengths of the Programme

Key strengths include a robust curriculum designed to address the critical skills gap within the cybersecurity sector. Graduates emerge not only with strong academic foundations, but also with practical competencies essential for effective cybersecurity management. The integration of academic expertise from a diverse consortium of higher education institutions in Europe with leading experts in cybersecurity, along with insights from industry partners, creates a rich learning environment tailored to the needs of various stakeholders.

To ensure flexible educational pathways that meet diverse learner and industry needs, the curriculum is designed to equip students with skills for various ENISA-defined job profiles in cybersecurity. A market analysis with industry partners identified specific competencies relevant to different roles, resulting in tailored curricula that prepare students for eight distinct job profiles. Additionally, the program supports students in acquiring relevant industry certifications alongside their academic degree, alongside support student services to enhance employability.

Additionally, the program's delivery through a centralized Digital Learning Platform enhances accessibility and flexibility, making advanced education in cybersecurity available to a broad audience. Its lean

facility and infrastructure requirements allow for a cost-effective model; current pricing strategies indicate that the 120 ECTS two-year full-time program may be offered at an initial price of €2,800 (only €700 per semester), while the three-year part-time program is priced slightly higher.

Flexible scheduling and remote education options broaden participation opportunities beyond traditional university students, making the program more inclusive for individuals with caretaking responsibilities, working professionals, and those with mobility restrictions. This approach not only fosters inclusivity, but also reduces commuting needs, potentially contributing to sustainability efforts.

Despite its affordability, the curriculum is cutting-edge in content and delivery, granting access to insights from leading cybersecurity scholars and real-world applications across Europe. This strategic alignment of affordability, accessibility, and high-quality content positions the program as a leader in advanced cybersecurity education, effectively preparing graduates to tackle the challenges of an evolving digital landscape.

Points for Attention

A critical focus for the program is the transition from an EU-funded project to a self-sustaining entity. The consortium is well-prepared for this transition, as outlined in the Cooperation Agreement. Initially led by UDS and UPB in close collaboration during the program's early implementation phase, the consortium is set to establish an independent legal entity to manage the program's financial and operational responsibilities post-EU funding. This entity will comprise key organizational units, including:

- **Executive Leadership**: Provides strategic direction.
- **Secretariat**: Handles administration and student fees.
- **Finance Department**: Manages revenue distribution and expenses.
- **Joint Admissions Board**: Oversees admissions.
- **Examination Board**: Ensures academic standards.
- **Quality Enhancement and Curriculum Development Committee**: Maintains curriculum quality.
- **Equality, Diversity, and Inclusion Board**.
- **Ad hoc committees**: Formed as needed.

These structures will ensure compliance with accreditation requirements and support the program's long-term sustainability, managing the distribution of costs, income and responsibilities among the partners. Pricing estimates suggest tuition fees may increase to around €5,600 for the two-year, full-time 120 ECTS program (approximately €1,400 per semester) after EU funding ends, still maintaining competitive pricing to support students with varying financial means.

As the program evolves, ongoing attention will be necessary to align with changing industry demands and technological advancements. Regular engagement with an established industry advisory board will be vital for adapting the curriculum to continuously meet real-world requirements and emerging trends. Survey-based annual module and program reviews will inform strategic adjustments. The Annual Program Review Report from the Quality Enhancement and Curriculum Development Committee will overview data for informed decision-making.

As the program is delivered entirely online, it's essential to focus on enhancing user experiences and providing comprehensive support. Regular feedback from students and faculty is collected to identify potential issues like exhaustion or loneliness, e.g., as monitored by the sample surveys. The program

leverages digital technologies, including gamification elements, to enhance engagement. Teachers receive ongoing feedback to improve their offerings. Both for students and faculty, on-site events and activities provide opportunities for in-person networking and collaborations. Additionally, comprehensive support services are integrated into the program to ensure a positive learning experience.

Finally, efforts will focus on attracting a diverse cohort of students and faculty, ensuring inclusivity and aiming for gender balance. The consortium's quality management program will monitor developments in this area, ready to identify and address any issues related to enrollment or critical in-class experiences, aiming to make the program a rich and beneficial experience for all learners.

Future Policy Options and Ambitions

Looking ahead, the program aspires to expand its reach, targeting over 2,500 graduates within the next four years. Strategic partnerships with European companies and SMEs will be pivotal in fostering a practical learning environment, facilitating internships, and ensuring that the program remains relevant to the needs of the market. By focusing on capacity building and training for both students and faculty, the Joint Master’s Programme will help develop a pipeline of qualified cybersecurity professionals, bolstering the long-term competitiveness and security of European industries.

To support job readiness, the Careers and Opportunities Support Service and the Employability Strategy will monitor and improve program effectiveness through feedback from students, graduates and continuous industry consultations.

The Digital4Security consortium will also implement a localization strategy, adjusting offerings to meet local market needs in target countries and regions. Initially, the program will be launched in countries with established university partners, leveraging their expertise to enhance reach. Local teams will adapt offerings with supplementary events, diverse pricing models, scholarships, and targeted communications.

Additionally, the consortium plans to accredit not only the entire program, but also selected modules as micro-credentials under national law, providing learners with greatest flexibility in tailoring their education.

In summary, the Joint Master’s Degree Programme in Cybersecurity Management and Data Sovereignty is set to become a cornerstone of advanced cybersecurity education in Europe, addressing current challenges while preparing graduates for future demands in a rapidly evolving digital landscape.

Annexes

Further documentation supporting the submission of the Self-Evaluation Report for accreditation of the Joint Master's Degree Programme in **Cybersecurity Management & Data Sovereignty** is provided as a set of annexes to this document.

Annex 1. Cooperation Agreement

Annex 2. Module Handbook

Annex 3. Study and Examination Regulations

Annex 4. Academic Staff CVs

Annex 5. Internal Quality Handbook

Annex 6. Student Handbook

Annex 7. Sample Degree Certificate

Annex 8. Sample Diploma Supplement

Annex 9. Sample Evaluation Questionnaires

Cooperation Agreement

Digital4Security
Shaping Europe's cyber future

Project details: Joint Master's Degree Programme
in Cybersecurity Management & Data Sovereignty (Digital4Security)

Project ID: 101123430

Call: DIGITAL-2022-SKILLS-03

Cooperation Agreement for the Establishment of a

Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty

between

Politehnica University of Bucharest (POLITEHNICA B.)
and
German University of Digital Science (German UDS)
and
National College Ireland (NCI)
and
Munster Technological University (MTU)
and
University of Brescia (UNIBS)
and
Brno University of Technology (BUT)
and
University of Rijeka (UNIRI)
and
Politechnic University of Milan (POLIMI)
and
Universidad Internacional de La Rioja (UNIR)
and
Vytauto Didziojo Universitetas(VMU)
and
Mykolas Romeris University (MRU)
and
Cergy Paris University (CY)
and
University of Koblenz (UNI KO)

Project details: Joint Master's Degree Programme
in Cybersecurity Management & Data Sovereignty (Digital4Security)

Project ID: 101123430

Call: DIGITAL-2022-SKILLS-03

About the Digital4Security project

The Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty is designed to create a highly innovative, effective, and sustainable training program for cybersecurity professionals. This program emerges from the DIGITAL4Security project, which addresses the urgent need for cybersecurity expertise within European Small and Medium Enterprises (SMEs) and other organizations, aiming to protect industries from cyber-attacks and safeguard economic prosperity. The project's central goal is to develop an innovative European Master's Programme in Cybersecurity Management & Data Sovereignty, equipping graduates with the technical, regulatory, and management skills required to combat existing and emerging cyber threats.

This contributes to the overarching aims of the DIGITAL Europe Programme by accelerating the progression of a large number of graduates through a dynamic stakeholder ecosystem, utilising an innovative pan-European online approach. In this approach, Higher Education Institutions (HEIs), Research Centres, Employment Services, and Industry collaborate to design, promote, deliver, and enhance an innovative Master's Programme. The master's programme will offer both part-time and full-time study options, integrating academic and industry content to fast-track students into high-demand cybersecurity roles, such as Cybersecurity Risk Manager and Chief Information Security Officer (CISO).

The Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty aims to enhance the cybersecurity skills of professionals through upskilling and reskilling. It offers flexible learning paths combining predominantly managerial and in addition technical content to meet industry needs. A focus on the development of advanced cybersecurity leadership skills, including critical assessment of principles, technologies, and practices relevant to modern enterprises allows participants to strategically apply knowledge to lead cybersecurity efforts across industries. Participants will be equipped to adapt to evolving threats, and bridge knowledge gaps through self-learning after successfully finishing their study program. The program emphasizes leadership in managing security initiatives, evaluating and mitigating cyber threats, making strategic decisions, and ensuring compliance with legal and regulatory frameworks, while fostering close collaboration with European companies, which ensures the program remains relevant to market demands. Aligned with the European Cybersecurity Skills Framework and the DIGITAL Europe Programme, it contributes to Europe's economic growth.

The modules will focus on the practical application of Cybersecurity Management & Data Sovereignty. They will incorporate academic and industry content to ensure that graduates are equipped with both theoretical knowledge and employment-ready digital skills, which will promote career success. Digital4Security promotes the attainment of industry-recognised certifications as an essential part of the learning pathway. The quality assurance process for the DIGITAL4Security Master's programme will be conducted in accordance with the European Approach for Quality Assurance of Joint Programmes. Online teaching and learning environments will utilise industry standard tools to enhance learning opportunities for part-time students and professionals already in employment. Additionally, it will include mentoring programmes with industry partners and industry-focused project-based learning.

The programme will be offered in two different formats to cater to diverse student cohorts: (1) a part-time MSc programme and (2) a full-time MSc programme. Additionally, modules may be offered as microcredentials to provide targeted upskilling opportunities, such as for professionals seeking specialized training in specific areas. These microcredentials do not need formal accreditation as derivatives of an officially accredited Master's Programme. We aim to launch multiple part-time and full-time cohorts over the 4-year project duration, with at least one part-time and two full-time cohorts completed within this period. The initial part-time and full-time cohorts will serve as pilots, with a cyclical review and enhancement process implemented annually.

The Digital4Security Consortium

The Digital4Security consortium is a partnership of 18 stakeholders (13 academic partners and 5 associated partners) led by Politehnica University of Bucharest, bringing together key industry, technology, and education stakeholders in the realm of cybersecurity and digitality in general in Europe. Its composition is presented in the following table.

Partners	Acronym
Politehnica University of Bucharest	POLITEHNICA B.
German University of Digital Science	German UDS
National College Ireland	NCI
Munster Technological University	MTU
University of Brescia	UNIBS
Brno University of Technology	BUT
University of Rijeka	UNIRI
Politechnic University of Milan	POLIMI
Universidad Internacional de La Rioja	UNIR
Vytautas Magnus University	VMU
Mykolas Romeris University	MRU
Cergy Paris University	CY
University of Koblenz	UNI KO

Associated Partners	Acronym
CEFRIEL SOCIETA CONSORTILE A RESPONSABILITA LIMITATA SOCIETA' BENEFIT	CEFRIEL
ATAYA & PARTNERS	ATAYA
SERVICENOW IRELAND LIMITED	ServiceNow
PROFIL KLETT D.O.O.	PROFIL KLETT
Red OPEN S.r.l.	ReD OPEN

Section 1. Purpose

A. This Cooperation Agreement represents the joint procedure for the provision of a 120 ECTS Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty (hereinafter referred to as the "degree programme"). This Agreement has been developed by the Partner Institutions in accordance with legislation in their respective jurisdictions and it establishes joint procedures and criteria for awarding a joint degree. The Agreement will come into effect in February 2025.

Without affecting the former, the Agreement is also intended to be in accordance with a multi-beneficiary grant agreement (hereinafter referred to as the "grant agreement") with the European Health and Digital Executive Agency (HADEA) within the framework of the Digital Europe Programme, Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, with respect to provision of funding for Project 101084013 - Digital4Security.

The objective of the present Agreement is to define how the Partner Institutions will cooperate from the academic year 2024/2025 to implement the degree programme. Subject to statutory rules and internal regulations of the partner institutions, students completing their studies under the terms of this Agreement will be awarded the Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty (120 ECTS).

B. The study programme, object of this Agreement, is implemented in observance of national laws and regulations in force in partner institutions' countries.

C. The partner institutions identified herein as degree-awarding partner institutions (see Section 3.D) are authorized to award a joint degree in an international joint study programme.

Section 2. Parties

A. The Cooperation Agreement is concluded by and between the following Parties:

1. **UNIVERSITATEA NATIONALA DE STIINTA SI TEHNOLOGIE POLITEHNICA BUCURESTI (POLITEHNICA B.)**, PIC 880988630, established in SPLAIUL INDEPENDENTEI 313 SECT 6, BUCHAREST 060042, Romania, and
2. **UNIVERSITY OF DIGITAL SCIENCE GGMBH (UDS)**, PIC 887596949, established in MARLENE-DIETRICH-ALLEE 14, POTSDAM 14482, Germany, and
3. **NATIONAL COLLEGE OF IRELAND (NCI)**, PIC 983034473, established in MAYOR STREET IFSC, DUBLIN 1, Ireland, and,
4. **MUNSTER TECHNOLOGICAL UNIVERSITY (MTU)**, PIC 892106673, established in ROSSA AVENUE BISHOPSTOWN, CORK T12 P928, Ireland, and
5. **UNIVERSITA DEGLI STUDI DI BRESCIA (UNIBS)**, PIC 999893946, established in PIAZZA MERCATO 15, BRESCIA 25121, Italy, and
6. **VYSOKE UCENI TECHNICKE V BRNE (BUT)**, PIC 999873091, established in ANTONINSKA 548/1, BRNO STRED 601 90, Czechia, and
7. **SVEUCILISTE U RIJECI (UNIRI)**, PIC 997640733, established in TRG BRACE MAZURANICA 10, RIJEKA 51000, Croatia, and
8. **POLITECNICO DI MILANO (POLIMI)**, PIC 999879881, established in PIAZZALEONARDO DA VINCI 32, MILANO 20133, Italy, and
9. **UNIVERSIDAD INTERNACIONAL DE LA RIOJA (UNIR)**, PIC 956152281, established in AVENIDA DE LA PAZ 137, LOGROÑO 26006, Spain, and
10. **VYTAUTO DIDZIOJO UNIVERSITETAS (VMU)**, PIC 999590627, established in K DONELAICIO G 58, KAUNAS LT-44248, Lithuania, and
11. **MYKOLO ROMERIO UNIVERSITETAS (MRU)**, PIC 996876082, established in ATEITIES G 20, VILNIUS 08303, Lithuania, and
12. **CY CERGY PARIS UNIVERSITE (CY CERGY PARIS)**, PIC 897499873, established in 33 BOULEVARD DU PORT, CERGY-PONTOISE 95011, France, and
13. **UNIVERSITAT KOBLENZ (UNI KO)**, PIC 999856407, established in UNIVERSITATSSTRASSE 1, KOBLENZ 56070, Germany.

B. Further parties can be added to this Agreement. The addition of new partners may require a review of the terms of this Agreement in alignment with Section 13.4. Hereinafter, the Parties to this Cooperation Agreement are collectively referred to as the "Partner Institutions" or interchangeably as "the Parties"; they are also referred to individually as "Partner Institution" or "Party".

C. All Partner Institutions are actively involved in the development, design, assessment, monitoring for quality assurance purposes, and collaborative delivery of programme modules on the Joint Master's

Degree Programme in Cybersecurity Management & Data Sovereignty (inclusive of any embedded programmes and associated micro-credentials).

D. Furthermore, Partner Institutions can fulfil one of two cooperative participation roles depending on whether or not i) a Partner Institution is recorded on the degree document as an awarding institution; or ii) a Partner Institution is not recorded on the degree document as an awarding institution, but is recorded on the Diploma Supplement as a contributing Partner Institution as per Section 2.C. Hereinafter, Partner Institutions fulfilling role i) are referred to as 'degree-awarding Partner Institutions'; Partner Institutions fulfilling role ii) are referred to as 'non degree-awarding Partner Institutions'. It is within the scope of this agreement that Partner Institutions can switch roles from a non-degree awarding Partner Institution role to a degree-awarding Partner Institution role, subject to the Partner Institution that is switching roles meeting all necessary national legislative requirements and the agreement of all other Parties.

E. In addition to the aforementioned, the Partner Institutions can have **associated partners** with a limited role in the implementation of the degree programme in the form of, but not limited to, knowledge and skills transfer, the provision of complementary courses or backing possibilities for secondment or placement. For contractual management issues, associated partners are not considered as part of the Cooperation Agreement since they have a more limited role in the implementation of the degree programme. Arrangements between the Partner Institutions and associated partners concerning the degree programme shall be regulated separately and must be in conformity with the requirements of this Agreement. The Secretariat, as described in Section 4.4, shall ensure that all Partner Institutions are informed about the contacts and separate arrangements with associated partners.

Section 3. Legal Framework

A. The Partner Institutions hereby agree as follows with regard to the activities described in the terms and conditions herewith. This Agreement shall specify the rights and obligations of the Partner Institutions concerning the delivery and running of the degree programme. All Partner Institutions are subject to the rules and regulations set up by this Agreement regarding both the responsibilities towards students and other parties to this Agreement.

B. For the duration of this agreement as defined in Section 13.7 and 13.8, this Cooperation Agreement establishes a 120 ECTS joint Master's degree programme, i.e. level 7 of the European Qualifications Framework, level 7 of the European Qualifications Framework for Lifelong Learning.

C. The Partner Institutions are subject to their own national legislative requirements and agree that they shall (at their own expense) co-operate and provide all necessary assistance as may be reasonably requested by any Partner Institution to enable compliance with such obligations.

D. For the duration of this agreement as defined in Section 13.7 and 13.8, all Partner Institutions shall ensure that the degree programme is correctly registered, shall ensure or strive that the degree programme is correctly accredited as a joint Master degree for 120 ECTS in their national jurisdiction in accordance with national regulations and shall duly inform each other of any developments regarding the accreditation status. The Partner Institutions will adjust the implementation of this Cooperation Agreement to any new legislation coming into force during the duration of the agreement.

E. The Partner Institutions agree to co-operate fully in relation to any audits, reviews, evaluations and quality assurance processes, monitoring, assessments, and reports undertaken by any Partner Institution and by any other relevant body or person as agreed by the Master's Board as defined in Section 4.3.

F. Compliance with EU General Data Protection Regulation (GDPR)
The Joint Admission Board, issuing universities alongside all partnering institutions, collectively assumes responsibility for adhering to the European Union General Data Protection Regulation (GDPR).

This entails:

1. Adaptation to GDPR: All academic partners must align their policies and practices with GDPR requirements.
2. Designation of Responsible Personnel: Each institution, in collaboration with the Joint Admission Board, must designate an individual responsible for overseeing student data protection.
3. Training and Awareness: Staff members handling personal data across all partners must undergo training on GDPR compliance, organized by the Joint Admissions Board.
4. Data Processing Agreements: Agreements between partners must ensure GDPR compliance when sharing personal data.

By jointly agreeing to this cooperation, the Joint Admission Board and partnering institutions affirm their collective commitment to GDPR compliance and the protection of students' data.

G. The Partner Institutions shall provide within five (5) working days of receipt of a request for assistance from any Partner Institution such information in its possession or power as may be reasonably requested to assist the Partner Institution to comply with its obligations under national legislation.

H. If for some reason the degree programme at one Partner Institution loses its accreditation to award the joint Master's degree according to its national law and regulations, the Institution shall be removed from this agreement pending new national accreditation. In this case an equivalent sustainable solution for the students will be provided by another partner institution.

Section 4. Programme Governance

4.1 Roles and Duties

A. **Programme Directors**: Each Partner Institution appoints at least one academic Programme Director. The Programme Director shall liaise with his or her counterparts in the other Partner Institutions on all matters concerning the degree programme and shall ensure that the degree programme at his or her Partner Institution is consistent with the joint agreements concerning the degree programme.

B. **Programme Coordinators**: The Programme Coordinator assists the Programme Director and carries out day-to-day administrative and technical tasks concerning the students, quality assurance, mobility in the degree programme and general matters related to programme delivery by the partner institutions. He or she liaises with the other Partner Institution Programme Coordinators and Programme Directors, students in the degree programme, and with external partners. In addition, the Programme Coordinators support the Secretariat and the Joint Programme Committee, as defined in Section 4.2.2 and Section 4.2.5 respectively, with the data collection system, information analysis and proposals and suggestions for the quality enhancement of the Master.

C. **Programme Faculty**: The academic teaching staff of the Partner Institutions and associated partners directly involved in the development and implementation of the degree programme.

D. **Issuing Institution**: The degree-awarding Partner Institution responsible for the issuing of the physical joint degree award, its diploma supplement, and any pertaining tasks on behalf of or in joint decision with the other degree-awarding Partner Institutions and non-degree-awarding Partner Institutions as described in this Agreement. The development of formal documentation relating to the joint degree award, the parchment, diploma supplement and any other formal documentation relating to the joint Master's degree programme shall be undertaken in consultation with, and subject to formal approval by, the Partner Institutions.

E. **Project Coordinator:** The Coordinator is responsible for:
   - Student Recruitment, Onboarding, and Support: Managing recruitment, onboarding, and support processes, including the use of digital platforms and supplementary events.
   - Industry Certifications & Micro-Credentials: Implementing industry certifications and micro-credentials.
   - Employability Programme: Establishing an employability programme for students.
   - European Mobility Programme: Facilitating student and lecturer mobility between institutions and companies.
   - Faculty Training Resources: Providing resources for faculty training and support.

In the early implementation phase, program coordination is led by Politehnica University of Bucharest (UPB) for the EU-funded project, with German UDS as implementation lead post-accreditation. German UDS will act as interim lead, working closely with UPB and the consortium to enable rollout from a country that can

support a fully online master's program. Following this, an independent legal entity shall be established to ensure the program's sustainable continuation post EU-funding.

4.2 Joint Governing Bodies

All governing bodies established by this Agreement and herein described which have responsibility for the various aspects of the joint Master's degree programme, shall be subject to the internal governance and management arrangements and oversight of the respective Partner Institutions. The following governing bodies are established:

- Master's Board of Directors,
- the Secretariat,
- the Project Coordinator
- the Joint Admissions Board,
- the Examination Board,
- the Joint Programme Committee,
- the Quality Enhancement and Curriculum Development Committee,
- and when required, ad hoc committees.

4.2.1 Programme Board of Directors

A. The Programme Board of Directors, hereinafter the Master's Board, shall comprise the Programme Directors that have been selected by each of the Partner Institutions to represent them on all matters concerning the degree programme within the limits of this Agreement. The Master's Board shall be responsible for general management, financial supervision, academic supervision, quality assurance, degree awarding and recognition issues, agreement changes, dispute resolution and student complaints. Additionally, the Master's Board is responsible for the system review, advice on policy developments for the joint degree programme, and to ensure the coherence and consistency of the concept of the programme.

B. The Programme Director of each Partner Institution shall be a voting member on the Master's Board.

C. The Master's Board establishes by consensus its own decision-making procedures and for which domains consensus shall not be required, unless stated otherwise in this cooperation agreement.

D. The Master's Board shall meet at least twice each year. Meetings may either be in person or held via electronically mediated systems or a combination of in person / electronically mediated.

E. In case of absence, a Programme Director should mandate a deputy to replace and represent him or her as a voting member in meetings of the Master's Board.

F. Minutes of the Master's Board meeting shall be distributed to all members of the Master's Board within fifteen days after the meeting. Any changes to the draft minutes must reach the Programme Secretariat

within one week after the distribution of the minutes. After this deadline, the Programme Secretariat shall produce and file a final version, a copy of which shall also be sent to all Programme Directors.

4.2.2 Programme Secretariat

A. The Secretariat shall have the responsibility for the overall daily operational and administrative management of the programme under the guidance and governance of the Master's Board.

B. The Secretariat shall be partly based at the Project Coordinator Institution, also designated as the Master's Secretariat, to support the coordination and day-to-day management of the programme and its support mechanisms, specifically tasks regarding quality assurance, application, selection and admission, student administration, and mobility coordination.

C. The Secretariat shall also include a wider group of Programme Coordinators (as detailed in Section 4.1/B). Each Partner Institution shall designate a representative member to serve on the Programme Coordinators group. These institutional representatives will collaborate with their counterparts from other partner institutions. They will provide administrative support to the Secretariat, addressing issues specifically related to the partner institution they represent.

D. The Secretariat shall also provide direct assistance for the Master's Board Meetings (including the preparation of minutes), maintaining the public website, and performing additional duties as delegated by the Master's Board.

4.2.3 Joint Admissions Board

A. Assisted by the Secretariat and under the supervision of the Master's Board, the Joint Admissions Board shall be responsible for the selection and admission of all students to the degree programme.

B. The Joint Admissions Board shall consist of one representative from each Partner Institution. The Partner Institution is responsible for appointing its representative in accordance with its own procedures and national regulations.

C. The Joint Admissions Board convenes physically or through electronically mediated systems at least once after each application deadline and can hold additional meetings until a selection and admission procedure is completed.

4.2.4 Examinations Board

A. The Examinations Board is headed by the Master's Board of Directors. The Master's Board is responsible for the overall quality and standards of the degree programme and for agreeing upon the academic standards. It monitors the partner institutions' compliance and is responsible for the degree programme being delivered to the highest academic standards.

B. The Examinations Board may be supplemented with additional nominees from Partner Institutions that have expertise in quality assurance and those who are responsible for programme examination administration.

C. Meetings of the Examinations Board shall convene after each programme examination session and after a provision of adequate time for grading and assessment of learners' exam scripts, project submissions, or other relevant coursework by programme faculty.

D. The Examinations Board shall deliberate cases, brought to its attention with at least one week notice. If the nature of the case brought to its attention demands a swift ruling, a special meeting may be arranged or written consultation of its members via electronically mediated systems instead.

E. All assessments are conducted in accordance with the jointly agreed policies and procedures for the degree programme as adopted by the Master's Board.

4.2.5 Joint Programme Committee

A. The Joint Programme Committee acts as advisor to the Master's Board of Directors. It is responsible for the system review and advice on policy developments for the joint degree programme.

B. For the duration of the funding period, the Joint Programme Committee meets physically at least once a year to ensure the coherence and consistency of the concept of the joint degree programme. Additional meetings, including those specified by the Internal Quality Handbook of the programme, can also be held via electronically mediated systems.

C. The Joint Programme Committee is composed of representatives from the Secretariat, Programme Coordinators, the Master's Board of Directors, and Faculty representatives.

4.2.6 Quality Enhancement and Curriculum Development Committee

A. The Quality Enhancement and Curriculum Development Committee, hereinafter the QECD Committee, is composed of at least one academic faculty member from each Partner Institution.

B. The QECD Committee prepares and implements on behalf of the Master's Board of Directors quality enhancement and curriculum development and reinforces the jointness of the degree programme adhering to the European Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG). The QECD Committee is accountable to the Master's Board.

C. The QECD Committee meets whenever called upon or whenever the periodic internal quality procedures as detailed in the Internal Quality Handbook of the Programme require, either in person or via electronically mediated systems.

D. The QECD Committee assists the Joint Programme Committee to evaluate the degree of achievement of learning objectives and the coherence of the programme and ensures that there are effective procedures for data collection, information analysis and proposals and the channelling of suggestions for improvement of the degree programme.

4.2.7 Ad-hoc Committees

A. The Master's Board can establish committees or task forces for specific assignments that fall outside the direct scope or capacity of the aforementioned joint governing bodies.

Section 5. Student Administration

5.1 Student Application, Selection, and Admission

The Study and Examination Regulations attached in annex to this Cooperation Agreement regulate the application, selection, and admission procedures in detail, including the eligibility and selection criteria, language qualification requirements, the joint application procedure, the admission procedure, and the Joint Admissions Board.

5.2 Joint Degree Application

A. The application procedure for the degree programme is jointly organised and implemented by the Partner Institutions in agreement with the Study and Examination Regulations.

B. The Secretariat, on behalf of the Partner Institutions, shall organise, receive, and process all applications for admission to the degree programme. All applications shall be processed through a centralised system.

C. Admission numbers and application deadlines are agreed among the partner institutions and made public in advance of the application process.

5.3 Selection and Admission

A. The Joint Admissions Board shall be responsible for the annual selection and admission of all students to the degree programme in accordance with the joint procedures and criteria specified in the Study and Examination Regulations attached in annex to this Cooperation Agreement.

B. The Master's Board shall be responsible for setting and reviewing the admission criteria in the Study and Examination Regulations according to and harmonized with the individual national law and regulations of the partner institutions. Due consideration shall be given to national requirements for admission of students.

C. No Partner Institution is obliged to admit a student in conflict with national legal requirements for admission.

D. The Secretariat shall assist the Joint Admissions Board with the selection and admission of all students on the degree programme.

5.4 Registration and Enrolment

A. The Secretariat shall be responsible for drawing-up the list of admitted students according to the timing agreed by the Master's Board and shall inform the Partner Institutions accordingly in a timely manner. The Secretariat shall prioritize maximizing student enrollment, while ensuring clear and flexible admission guidelines are established to facilitate effective student admission processes, thereby guaranteeing that enrolled students meet all eligibility criteria.

B. Prior to a learner's enrolment in the degree programme, the accepted student and a representative of the Master's Board shall sign a Student Agreement covering the academic, financial, administrative, behavioural, and other relevant aspects related to the degree programme and, if applicable for scholarship holders, the scholarship management. In addition, the Student Agreement shall include the Study and Examination Regulations (detailing the requirements for successful acquisition of ECTS credits, the consequences in case of failure to acquire them, and the grading system), as well as information about the services provided to the student, and details related to health and social security, mobility requirements, and project, exam and graduation rules to the extent described in the online Student Handbook. The Partner Institutions will take care that the student is informed of any updates in this information.

C. The Secretariat shall assist the Joint Admissions Board with the selection and admission of all students on the degree programme.

D. All learner registrations and enrolments shall be processed through a centralised system in agreement with the regulations of the Issuing Institution and the respective national legal requirements.

E. In terms of module-level teaching and learning, learner mobility will predominantly be virtual, with learners enrolling on modules that will be delivered by Faculty members from across the partner institutions.

5.5 Examination of Students

A. The Study and Examination Regulations attached to this Consortium Agreement regulate the examination and assessment of students of the degree programme, including joint agreements on the order of examinations, assessment methods and criteria, grading, the joint conversion table for grades, access to information on grading, resists and re-assessments, functional disorders and handicaps, unfair practice, and fraud.

B. Partner Institutions shall conduct examinations and assessments in accordance with their own policies and procedures, provided they align with those established by the Master's Board and detailed in the Study and Examination Regulations of the Consortium, and are compliant with national law.

C. All modules are weighted according to the ECTS system and in conformity to national regulations on this. Partner Institutions accept differences in national regulations among the Partner Institutions concerning awarding ECTS credits and they recognise the number of ECTS credits awarded by Partner Institutions for the degree programme without further conversion.

D. Where required, all grades shall be converted and recognised in conformity with the joint conversion table for grades as established in the Study and Examination Regulations attached in annex to this Agreement.

5.6 Student Records

A. Each Partner Institution keeps appropriate records of the students attending its programme, and provides students and partners the certification of a student's performance on request. It is a requirement that all students are able to access their records via the programme's online platform. The programme's online platform will provide the necessary supporting features to fulfil this requirement.

B. Each Partner Institution shall be responsible for keeping accurate records of their students and for transferring records in a timely fashion after examination to the central records of the Issuing Universities and the Secretariat, as well as to Partner Institutions that require a full academic record of a given student to award the joint degree according to their legislation.

C. The communication shall be undertaken by the registrar offices of each university, or their equivalent, through a transcript of records released in English at minimum.

5.7 Final Degree and Joint and Mutual Recognition

A. Each Partner Institution formally recognises the modules offered within the joint degree programme and the credits awarded.

5.8 Joint Degree Award and Diploma Supplement

A. Each student who successfully completes the degree programme as described in the Study and Examination Regulations and who has fulfilled the requirements of the applicable national legislations shall receive a joint Master's degree testified by a joint diploma on behalf of the degree awarding Partner Institutions involved in the provision of the degree programme to that student.

B. Each joint degree award is accompanied by a diploma supplement presenting the details of the student's academic programme and academic achievement, following the template developed by the European Commission, the Council of Europe and UNESCO/CEPES and adapted to any further specifications in national legislation where applicable. Non-degree-awarding partner institutions are also listed on the diploma supplement as collaborative partners.

C. The Issuing Universities, as defined in article 4.1.D, shall be responsible for:

- delivering and issuing a single joint degree award, the diploma supplement, and their duplicates on behalf of or in joint decision with the Partner Institutions involved in the provision of the joint degree programme to that student; and
- registering the official joint degree according to national law and custom within its country.

D. The Partner Institutions shall:

- confer the right to issue and deliver the joint degree award and/or the diploma supplement on their behalf to or in joint decision with the Issuing Institution as defined in article 4.1.D;
- recognise the joint degree award and/or the diploma supplement issued by the Issuing Institution on their behalf or based on a joint decision;
- be responsible, if applicable, for submitting the full transcript of records of the student's degree programme followed at its location; and
- be responsible, if applicable, for registering the official joint degree according to national law and custom within its country.

E. The degree-awarding Partner Institutions agree that this Cooperation Agreement in combination with their national legislation provide sufficient legal basis to start issuing joint degree awards as a consortium.

F. The joint degree awarded shall clearly state that it is a Joint Master's Degree in Cybersecurity Management & Data Sovereignty. It shall also clearly indicate the institutions on behalf of which the degree is being awarded and shall be issued according to this Cooperation Agreement.

G. The degree-awarding Partner Institutions hereby allow each other to use their crests and logos on the joint degree award and diploma supplement issued under this Cooperation Agreement, when the joint degree award and diploma supplement is issued on their behalf or in joint decision, or when national regulations require the Issuing Institution to indicate the group of partner institutions on the document.

H. The contributing non-degree awarding Partner Institutions hereby allow that their institution be recorded on the diploma supplement issued under this Cooperation Agreement, when the joint degree award and diploma supplement is issued on their behalf or in joint decision, or when national regulations require the Issuing Institution to indicate the group of partner institutions on the document; i.e., Section 2.4 of the Diploma Supplement 'Name and status of institution (if different from 2.3) administering studies (in original language)' shall include the names of the non-degree awarding Partner Institutions.

Section 6. Staff

6.1 Teaching and Administrative Staff

A. The Partner Institutions shall be responsible for appointing sufficient and appropriately qualified staff to deliver the various elements of the degree programme specified in this Cooperation Agreement and the Study and Examination Regulations.

B. Partner Institutions involved in the delivery of the degree programme are responsible for ensuring that their teaching staff are competent in the language of instruction specified in the Study and Examination Regulations for the degree programme at the Partner Institution.

C. The Consortium and its Partner Institutions endeavour to involve renowned scholars, experts and professionals in the field of the Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty to contribute to and further enhance the quality of the degree programme. Such involvement may include mobility of scholars/guest lecturers and staff members across the Partner Institutions themselves, between the Partner Institutions and associated partners, as well as inward mobility from outside the Consortium, with a clear link to the degree programme.

6.2 Staff Mobility

A. The Partner Institutions shall regulate the reception and/or employment of faculty members and administrative staff intended to participate in mobility under this Agreement, in conformity with their regulations and national law, where required and applicable.

B. Personnel covered by this Agreement shall continue to comply with the contractual obligations of their originating university and shall continue to receive their due remuneration and benefit from the rights that they are entitled to for their legal position, according to the legislative norms existing in the country of the originating university. In each case, the originating university shall consider the duration of the stay as an ordinary service period, for all intents and purposes.

Section 7. Quality Assurance

A. The Master's Board is responsible for the overall quality and standards of the degree programme. It shall monitor compliance of Partner Institutions with this Agreement and it shall be responsible for ensuring that the degree programme is delivered to the highest academic standards. For this purpose, the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG) shall serve as a reference. Accreditation and external review of the programme will follow the European Approach for Quality Assurance of Joint Programmes approved by the EHEA ministers in May 2015.

B. The QECD Committee assists the Master's Board in its Quality Assurance tasks and responsibilities including, but not limited to, the implementation of quality enhancement and curriculum development measures throughout the Consortium.

C. The ultimate responsibility for academic standards in each Partner Institution rests with the representative of that Partner Institution on the Master's Board.

D. Quality Assurance shall be based on both internal and external assessment measures, involving the relevant stakeholders in the degree programme.

E. External Quality Assurance shall comprise at least the required national accreditation based on the European Approach, but also the quality reviews for the European Commission and any other external assessments agreed upon by the Master's Board. In addition, every two years, the International Industry Advisory Board shall provide audit reports.

F. The Quality Assurance Framework outlines internal quality oversight, assessment procedures, and the relevant participation of degree course governing bodies. It describes and provides references for the methods and tools used to assess the degree program's modules, mobility, integration into the labour market, general satisfaction, and other quality-related factors.

Section 8. Programme Information

A. The Secretariat shall ensure that the online Student Handbook is updated and that its contents are in line with agreements sanctioned by the Master's Board.

B. The Secretariat shall ensure that module descriptions are up to date and complete and that they are publicly accessible on the master program website.

C. The Secretariat together with the partner institutions shall ensure that the materials are available on the teaching Platform.

Section 9. Financial Management

9.1 Financial Arrangement

A. Partner Institution POLITEHNICA B. shall be responsible for financial management, in collaboration with the German University of Digital Science as interim lead of the program implementation post accreditation. The signatories to the Cooperation Agreement authorise these institutions to handle financial management on their behalf. The General Secretariat shall have overall responsibility for the financial management of the degree programme, including the administration and intake of student participation costs, the management and distribution of scholarships and Erasmus Mundus Joint Master Degree (EMJMD) scholarships, as well as managing all other income and general expenditures in relation to the Consortium.

B. The signatories to the Cooperation Agreement agree to the allocation of funds for the administrative structures (see Section 4) and they agree to the redistribution scheme of centrally collected participation costs to the respective universities, as described in greater detail in the Digital4Security Consortium agreement. How the profit will be generated, collected, and distributed to the partners will be established as part of the Sustainability strategy. This will be reflected in an amendment to the Digital4Security Consortium Agreement and Cooperation Agreement. The Project Coordinator Institutions (POLITEHNICA B. and German UDS as interim lead for the program rollout) and the Issuing Universities (Joint Examinations Office) shall be responsible for the management of the consortium and of the joint programme according to a predesignated task division.

9.2 Student Participation Costs

A. The Master's Board can, subject to the approval of the Partner Institutions and the Digital4Security Consortium, agree to amend the participation costs to be charged to students.

B. The participation costs shall be quoted in Euros and shall be applied to all Partner Institutions.

C. Students pay ca. € 2800 (two thousand eight hundred euros) for the full-time programme, and ca. €4620 (four thousand six hundred and twenty euros) for a three-year part time programme, participation costs for the entire 120 ECTS programme for the nominal study period, whether European or non-European. These prices may be adjusted, but aim to remain highly competitive, making the program accessible to a wide range of students with varying financial capabilities. The student participation costs are to be paid to the Project Coordinator for the standard duration of the degree programme, including support in administrative and organisational issues by the consortium partners, any potential costs for enrolment at the consortium partner's institutions, all examinations and the issuing of the final diploma.
As the program progresses, the pricing strategy will be continuously reviewed, especially with the eventual phase-out of the current 50% EU co-funding by October 2026. By this time, fees are expected to shift toward the higher end of the range to ensure financial sustainability, with average costs potentially doubling, such as €5600 for the entire 120 ECTS two-year full-time Master's program instead

of the initial €2800. We will be monitoring the costs of the delivery of the Masters and adapt the fees accordingly.

D. Student participation costs do not cover accommodation, travel to and from partner universities and travel documents (visa, passport) included within the framework of the mobility programme or any costs beyond the standard duration of the degree programme. Any costs beyond the standard duration of the degree programme shall be levied at the standard rate applicable to the programme.

E. Students that receive a Diversity Programme grant shall receive a fee waiver for the tuition fees.

Section 10. Reporting

A. The Master's Board, with the assistance of the Secretariat and all Partner Institutions, shall be responsible for submitting all required reports and for reporting to the European Commission, the Consortium, and other relevant bodies.

B. The Master's Board, with the assistance of the Secretariat and all Partner Institutions, shall be responsible for maintaining, during the term of this Agreement and for five years after its termination or expiry, full and complete records relating to the degree programme.

Section 11. Intellectual Property Rights/Results

11.1 Specific Provisions for Access Rights to Module and Curricula Materials

The access rights to module and curricula materials produced within the Project are governed by Grant Agreement Article 16.4 and its Annex 5, Section Ownership of results. Consortium Parties are granted the freedom to Share and Adapt the materials, even for commercial purposes. However, they must give appropriate credit, provide a copyright notice, license notice, disclaimer, and include a link to the material. If changes are made, it should be indicated. Upon request, in cases of collection or adaptation, references to the author and licensor can be removed to the extent practicable. This is governed by the Digital4Security Consortium Agreement. Additionally, when a Consortium Party delivers materials, they should provide the coordinator with written proof or verification of awareness of the content being sent, ensuring its proper referencing and shareable nature.

11.2 Ownership of Results

A. Results are owned by the Party and/or by the Party's researchers that generates them pursuant to each Party' s national laws or intellectual property policy. If the researchers of a Party are entitled to claim rights to the Results pursuant to national laws, the Party concerned must ensure that the researchers comply with the obligations under the Grant Agreement and the Consortium Agreement.

B. Joint ownership is governed by Grant Agreement Article 16.4 and its Annex 5, Section Ownership of results, with the following additions:
Unless otherwise agreed:
- each of the joint owners shall be entitled to use their jointly owned Results for non-commercial research and teaching activities on a royalty-free basis, and without requiring the prior consent of the other joint owner(s).
- each of the joint owners shall be entitled to otherwise Exploit the jointly owned Results and to grant non-exclusive licenses to third parties (without any right to sub-license), if the other joint owners are given: (a) at least 45 calendar days advance notice; and (b) fair and reasonable compensation.

C. The joint owners shall agree on all protection measures and the division of related costs in advance.

11.3 Transfer of Results

A. Ownership of Result/Transfer of ownership: Each Party may transfer ownership of its own Results, including its share in jointly owned Results, following the procedures of the Grant Agreement Article 16.4 and its Annex 5, Section Transfer and licensing of results, sub-section "Transfer of ownership".

B. Third Parties: Each Party may identify specific third parties it intends to transfer the ownership of its Results to in Attachment (3) of this Consortium Agreement. The other Parties hereby waive their right to prior notice and their right to object to such a transfer to listed third parties according to the Grant Agreement Article 16.4 and its Annex 5, Section Transfer of licensing of results, sub-section "Transfer of ownership", 3rd paragraph.

C. Inform other Parties: The transferring Party shall, however, at the time of the transfer, inform the other Parties of such transfer and shall ensure that the rights of the other Parties under the Consortium Agreement and the Grant Agreement will not be affected by such transfer. Any addition to Attachment (3) after signature of this Consortium Agreement requires a decision of the General Assembly.

D. Mergers and Acquisitions: The Parties recognise that in the framework of a merger or an acquisition of an important part of its assets, it may be impossible under applicable EU and national laws on mergers and acquisitions for a Party to give at least 45 calendar days prior notice for the transfer as foreseen in the Grant Agreement.

E. Obligations: The obligations above apply only for as long as other Parties still have - or still may request – Access Rights to the Results.

11.4 Dissemination

A. Confidentiality obligations: For the avoidance of doubt, the confidentiality obligations set out in Section 12 apply to all dissemination activities described in this Section 11.4 as far as Confidential Information is involved.

B. Dissemination of own (including jointly owned) results: During the Project and for a period of 1 year after the end of the Project, the dissemination of own Results by one or several Parties including but not restricted to publications and presentations, shall be governed by the procedure of Article 17.4 of the Grant Agreement and its Annex 5, Section Dissemination, subject to the following provisions:

- Provision of prior notice: Prior notice of any planned publication shall be given to the other Parties at least 7 calendar days before the publication. Any objection to the planned publication shall be made in accordance with the Grant Agreement by written notice to the coordinator and to the Party or Parties proposing the dissemination within 30 calendar days after receipt of the notice. If no objection is made within the time limit stated above, the publication is permitted.
- Justification of an objection: An objection is justified if
    a) the protection of the objecting Party's Results or Background would be adversely affected, or
    b) the objecting Party's legitimate interests in relation to its Results or Background would be significantly harmed, or
    c) the proposed publication includes Confidential Information of the objecting Party.

  The objection must include a precise request for necessary modifications.

- Objection raised: If an objection has been raised the involved Parties shall discuss how to overcome the justified grounds for the objection on a timely basis (for example by amendment to the planned publication and/or by protecting information before publication) and the objecting Party shall not unreasonably continue the opposition if appropriate measures are taken following the discussion.
- Objecting Party: The objecting Party can request a publication delay of not more than 90 calendar days from the time it raises such an objection. After 90 calendar days the publication is permitted, provided that the objections of the objecting Party have been addressed.

C. Dissemination of another party's unpublished results or background: A Party shall not include in any dissemination activity another Party's Results or Background without obtaining the owning Party's prior written approval unless they are already published.

D. Cooperation obligations: The Parties undertake to cooperate to allow the timely submission, examination, publication and defence of any dissertation or thesis for a degree that includes their Results or Background subject to the confidentiality and publication provisions agreed in this Consortium Agreement.

Section 12. Confidentiality and Non-disclosure of Information

12.1 Confidential Information

A. All information in whatever form or mode of communication, which is disclosed by a Party (the "Disclosing Party") to any other Party (the "Recipient") in connection with the Project during its implementation and which has been explicitly marked as "confidential" at the time of disclosure, or when disclosed orally has been identified as confidential at the time of disclosure and has been confirmed and designated in writing within 15 calendar days from oral disclosure at the latest as confidential information by the Disclosing Party, is "Confidential Information".

12.2 Duration

A. The Recipient hereby undertakes in addition and without prejudice to any commitment on non-disclosure under the Grant Agreement, for a period of 5 years after the final payment of the Granting Authority:
   - not to use Confidential Information otherwise than for the purpose for which it was disclosed;
   - not to disclose Confidential Information without the prior written consent by the Disclosing Party;
   - to ensure that internal distribution of Confidential Information by a Recipient shall take place on a strict need-to-know basis; and
   - to return to the Disclosing Party, or destroy, on request all Confidential Information that has been disclosed to the Recipients including all copies thereof and to delete all information stored in a machine-readable form to the extent practically possible. The Recipient may keep a copy to the extent it is required to keep, archive, or store such Confidential Information because of compliance with applicable laws and regulations or for the proof of on-going obligations provided that the Recipient complies with the confidentiality obligations herein contained with respect to such copy.

12.3 Cover

A. The Recipient shall be responsible for the fulfilment of the above obligations on the part of its employees, or third parties involved in the Project and shall ensure that they remain so obliged, as far as legally possible, during and after the end of the Project and/or after the termination of the contractual relationship with the employee or third party.

12.4 Exclusions

A. The above shall not apply for disclosure or use of Confidential Information, if and in so far as the Recipient can show that:
   - the Confidential Information has become or becomes publicly available by means other than a breach of the Recipient's confidentiality obligations;
   - the Disclosing Party subsequently informs the Recipient that the Confidential Information is no longer confidential;

- the Confidential Information is communicated to the Recipient without any obligation of confidentiality by a third party who is to the best knowledge of the Recipient in lawful possession thereof and under no obligation of confidentiality to the Disclosing Party.
- the disclosure or communication of the Confidential Information is foreseen by provisions of the Grant Agreement;
- the Confidential Information, at any time, was developed by the Recipient completely independently of any such disclosure by the Disclosing Party;
- the Confidential Information was already known to the Recipient prior to disclosure, or
- the Recipient is required to disclose the Confidential Information to comply with applicable laws or regulations or with a court or administrative order, subject to the provision Section 12.6 hereunder.

12.5 Recipient's Duty of Care

A. Each Recipient shall promptly inform the relevant Disclosing Party by written notice of any unauthorised disclosure, misappropriation, or misuse of Confidential Information after it becomes aware of such unauthorised disclosure, misappropriation or misuse.

12.6 Requirement to Disclose Confidential Information in Certain Circumstances

A. If any Recipient becomes aware that it will be required, or is likely to be required, to disclose Confidential Information to comply with applicable laws or regulations or with a court or administrative order, it shall, to the extent it is lawfully able to do so, prior to any such disclosure:
   - notify the Disclosing Party, and
   - comply with the Disclosing Party's reasonable instructions to protect the confidentiality of the information.

Section 13. This Agreement

13.1 Contractual Relationship

A. This Agreement constitutes a contractual relationship between the Parties which shall exist only for the purposes set out in Section 1 of the present Agreement. This Agreement and its annexes constitute the entire agreement, and the Parties acknowledge that in entering into this Agreement no Party relies on, and shall have no remedy in respect of, any statement, representation, warrant or understanding, however made, other than as expressly set out in this Agreement.

B. This Agreement is not intended to create, nor should it be construed as creating a corporation, agency or partnership (whether general or limited), or any legal entity or continuing relationship or commitment between the Parties other than as expressly contained in this Agreement. There will be no sharing of profits or losses among the Parties.

C. Non-enforcement of any provision of this Agreement shall not constitute a waiver or precedent in respect of that or any other provision at any other time or by any other Party.

D. If any provision (or part of a provision) included in this Agreement is found to be illegal, void or unenforceable, in whole or in part, then such provision shall be severed from the rest of this Agreement and the remainder of this Agreement shall continue to have full force and effect for all intents and purposes of the law.

13.2 Transitional Provisions

A. The Parties agree to start a test phase of the programme by February 2025.

B. The Parties agree to fully start the Joint Master's Degree Programme in Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty, as governed by this Agreement, by October 2025.

C. Notwithstanding the previous clause, a Party may request an exemption from implementing certain parts of this Agreement if national legislation, university regulations or administrative procedures prevent implementation by October 2025, though under the condition that the other Parties agree with such an exemption and under the condition that the Cooperation Agreement and its annexes are fully adhered to by October 2025.

13.3 Development and Sustainability

A. In terms of excellence, course integration, the joint nature of the endeavour under this Agreement and financial viability, the Partner Institutions strive to develop and implement the degree programme in such a way that the degree programme can still be started, even if no EU funding should become available, and that it can exist beyond the EU funding period.

B. The Partner Institutions intend to secure financial sustainability beyond EU funding by:
   - committing 'in kind' resources that underpin the consortium partnership, enabling it to continue as an international network in the future; and
   - supporting the institutional embedding of the degree programme in the consortium partnership and at the Partner Institution itself in all necessary aspects.

C. The Consortium intends to secure sustainability in terms of finances and excellence of the degree programme by:
   - developing a portfolio approach to sources of finance, including the possibilities of non-EU scholarships for students;
   - supporting the students in minimising the associated costs and overheads for students of the degree programme;
   - periodically reviewing the degree programme and adapting it to deliver interdisciplinary multi-skilled graduates that respond to the Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty needs of industry;
   - increasing the involvement of relevant actors from industry in the degree programme, for example in the form of strategic partnerships;
   - advancing an integrated communication strategy for marketing the degree programme and involving alumni, networks, European and national agents in targeting different audiences of the degree programme;
   - pursuing and adhering to Erasmus Mundus as a brand of excellence for the degree programme on a global level;
   - constantly improving the strategic positioning at global level and performing a leading and innovating role in the global higher education market.

13.4 Amendments, Communications and New Partners

A. No change, alteration, modification or addition to this Agreement shall be valid unless agreed in writing and properly executed by the Parties hereto.

B. Any demand notice or other communication given or made under or in connection with this Agreement shall be in writing.

C. Subject to the approval of the Partner Institutions, the Master's Board can adopt and revise the Study and Examination Regulations and Internal Quality Handbook as attached to this Cooperation Agreement, as well as the online Student Handbook, without requiring a renewal of this Cooperation Agreement.

D. The consortium partnership, through its Master's Board, shall consider requests from potential partner institutions to become members of the consortium partnership. The addition of a new partner institution shall be regulated through an amendment to this Agreement, signed by the legally authorised representative of the existing Partner Institutions and the new Partner Institution.

13.5 Dispute Resolution

A. In the event of any dispute between the Parties regarding this Agreement, the details of the circumstances of any such dispute shall be communicated in writing by the Party alleging the same to the other Party/Parties, which communication shall also be copied to the Master's Board.

B. In the event of any dispute between the Parties regarding this Agreement, the Parties agree to attempt to reach an amicable settlement in good faith, which amicable settlement shall attempt to be facilitated by the Master's Board.

C. In the event that such attempt is unsuccessful, such dispute shall be resolved through a "Dispute Resolution Panel", being a three-person panel composed as follows:
   - The claimant and the respondent (or, in the case of multiple claimants and/or respondents, the multiple claimants, jointly, and/or the multiple respondents, jointly) shall each nominate one panel member. The nominated members shall appoint a third panel member, who also shall serve as the chairperson of the Dispute Resolution panel.

D. The Dispute Resolution Panel so constituted shall set its own rules of procedure and adjudicate the matter submitted to it.

E. The decision of the Dispute Resolution Panel shall be final, and upon it being communicated to the Parties, they shall abide by it forthwith as far as legally possible.

13.6 Application of Laws

A. Any dispute arising out of, or in connection with, this Agreement, including any question regarding its existence, validity, or termination, if not resolved by mutual amicable settlement or by means of a Dispute Resolution Panel between the Parties within a reasonable time, being no more than a total of three months, shall be subject to:
   - the national law of the Partner Institution wherein the conflict originated; or
   - should the former option not be applicable, the national law of the Award Issuing Partner.

B. Notwithstanding the previous clauses, the application of laws shall be such that legislation of the Parties involved is accommodated to the maximum extent possible.

13.7 Termination

A. Parties to this Agreement shall each be entitled to terminate their commitment to this Agreement through a phased withdrawal, for any reason, by giving at least twelve (12) months' notice in writing to the Master's Board prior to the 31st of August of any given year during the applicability of this Agreement.

B. The Master's Board may require a Party to terminate its commitment to this Agreement if that Party persistently does not fulfil its obligations and requirements as outlined in this Agreement.

C. In the event of a Party withdrawing from the Consortium, the Master's Board shall manage the phased withdrawal, respecting the interests of the enrolled students and ensuring the conditions for the effective continuation of their studies.

D. Any Party wishing to terminate its commitment shall agree upon a phased withdrawal plan, during which its legal obligations to each student must be analysed, assessed, and reported to the Master's Board. Should the Party be unable to honour its commitment to its students during the course of its withdrawal, arrangements shall be made to transfer the obligations to another Partner Institution. This may involve, among others, the transfer of funds between the Parties involved, for such purpose.

13.8 Duration

A. This Agreement shall apply for the period 1 October 2025 to 30 September 2030.

13.9 Signature Pages

A. Attached to this Agreement are signature pages whereby each legally authorised partner institution representative signs together with the legally authorised representative of the Coordinating Institution, thus agreeing to enter into this Agreement. Such signature pages are considered as part and parcel of this Agreement.

B. The Signature Page is done in two original copies of which one shall be kept by Schuman Associates in Brussels, Belgium, one shall be kept by the Coordinating Institution.

C. The Coordinating Institution shall provide duplicates of this Agreement and its signed signature pages to all Parties concerned.

Annexes

Annex 1. not applicable

Annex 2. Module Handbook

Annex 3. Study and Examination Regulations

Annex 4. Academic Staff CVs

Annex 5. Internal Quality Handbook

Annex 6. Student Handbook

Annex 7. Sample Degree Certificate

Annex 8. Sample Diploma Supplement

Annex 9. Sample Evaluation Questionnaires

Module Handbook

Digital4Security
Shaping Europe's cyber future

Project details: Joint Master's Degree Programme
in Cybersecurity Management & Data Sovereignty (Digital4Security)

Project ID: 101123430

Call: DIGITAL-2022-SKILLS-03

Table of Contents

Overview

Welcome to the Module Handbook of the DIGITAL4Security Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty. Digital4Security is a ground-breaking pan-European master's program aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. This €20m industry-led Master's, supported by funding from the DIGITAL Europe Programme, is a four-year initiative that comprises a Consortium comprising 34 partners spanning 14 countries. This master program will provide comprehensive knowledge of cybersecurity management, regulatory compliance, and technical expertise to European SMEs and companies.

Educational Philosophy and Approach

At the heart of DIGITAL4Security lies a commitment to a competency-based educational model that merges rigorous academic standards with practical, industry-relevant skills. This approach is informed by the latest curricular developments, which advocate for a synthesis of knowledge and competency models to foster a holistic learning environment.

The DIGITAL4Security Consortium is the backbone of our programme, embodying a shared vision of creating a centralised hub for advanced digital skills learning. This partnership among Europe's leading education institutions, research centres, and industry stakeholders underscores our commitment to a collaborative, interdisciplinary approach to digital education.

The Digital4Security curriculum is grounded in a rigorous needs analysis process involving all of our Consortium partners. The programme will blend academic and industry content to ensure graduates are equipped with both theoretical and job-ready cyber skills to fast-track employment. The programme will be academically accredited at a European and international level, with micro-credentials for each module, and industry certification through industry partners.

Flexibility and Inclusivity

Understanding the diverse needs of our student base, DIGITAL4Security offers a flexible, modular learning platform accessible to individuals from various sectors and backgrounds. This inclusivity extends to our delivery model, which combines online learning with physical workshops, seminars, and networking events. Our aim is to make advanced digital education accessible and affordable to the widest possible audience, fostering gender equality, ethnic diversity, and reducing unemployment among disadvantaged groups.

Vision for the Future

As we embark on this journey, DIGITAL4Security stands not just as an educational programme, but as a movement towards bridging the digital skills gap in Europe. Through academic excellence, industry collaboration, and a forward-looking curriculum, we aim to empower our students with the knowledge, skills, and professional dispositions necessary for success in the digital age.

Our engagement with the European Commission and participation in high-profile digital skills events underscore our commitment to this mission. We are poised to enrol our inaugural cohort of students, marking the beginning of a new chapter in European digital education.

We invite you to join us in this transformative endeavour, as we work together to shape the digital future of Europe.

This document contains Module Descriptors for each of the modules offered as part of the programme of study for the Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty. This document can be consulted for detailed information about each of the modules.

Yours truly,

The DIGITAL4Security Consortium

A.I. & Emerging Topics in CyberSecurity

Module designation	*A.I. & Emerging Topics in CyberSecurity*
Semester(s) in which the module is taught	*3*
Person responsible for the module	*Pejman Najafi <pejman.najafi@exasec.de>*
Language	*English*
Relation to curriculum	*Compulsory / elective / specialisation*
Teaching methods	*Lecture, self-organized learning (flipped classroom), tutorial, hand-on, seminar/discussions, case study, guest lectures.*

Workload (incl. contact hours, self-study hours)	*Total workload: 250 h*
	• *Contact hours: 60 h*
	  o *Lecture: 24 h*
	  o *Hands-on/Tutorials: 12 h*
	  o *Seminar/discussion & guest-lecture: 12 h*
	  o *Flipped classroom: 12 h*
	• *Private study: 190 h*

Credit points	*10 ECTS*
Required and recommended prerequisites for joining the module	1. *Security Operations* 2. *Machine Learning and Deep Learning in Cybersecurity* 3. *Ethical Hacking & Penetration Testing*
Module summary	*The module delves into AI and its impact on cybersecurity, highlighting its offensive and defensive applications. Using both lectures and flipped classroom sessions, students will learn key AI concepts and their applications in today's Security Operations Centers (SOCs). Finally, they will apply their learning in a group project, developing AI-powered cyber defense or attack scenarios.*
Module objectives/intended learning outcomes	*Knowledge* • Gain foundational knowledge in data science and engineering relevant to cybersecurity. • Acquire basic knowledge of Generative AI and Large Language Models (LLMs). • Comprehend the core principles of cyber defense and the role of Security Operations Centers. • Identify security issues associated with AI models, such as vulnerabilities, weaknesses, and adversarial threats. • Understand the primary challenges faced when integrating AI into cybersecurity, including data labeling, explainability, and trust issues. *Skills*

	• Perform research and articulate emerging trends in AI and cybersecurity. • Design and develop AI-driven solutions for real-world cybersecurity challenges, demonstrating proficiency in both offensive and defensive applications. *Competences* • Critically evaluate the strengths, and limitations of AI applications in cyberdefense. • Identify the potential misuse of AI by adversaries to automate and enhance TTPs. • Assess ethical and regulatory implications for the responsible use of AI in cybersecurity, addressing privacy concerns, bias mitigation, and compliance across various cultural and regulatory contexts. • Anticipate upcoming challenges and opportunities in cybersecurity and propose innovative solutions to address them.
Content	*--Prerequisites & recap of required knowledge--* **Week 1: Security Operations & Cybersecurity Foundations** *Summary*: Recap the essentials of cybersecurity, focusing on SOC operations and using the NIST Cybersecurity Framework as a reference. Bring students up to speed on fundamental concepts and ensure consistent prerequisite knowledge. *Lecture Content:* • NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover, Govern) • Key SOC operations: vulnerability management, threat detection, incident response, red teaming, … • SOC tools/technologies: SIEM, SOAR, IDS/IPS, EDR/NDR/XDR, TIP, … • Standards and frameworks: NIST CSF, MITRE ATT&CK, CIS • Data in SOC: Types, Values, and Significance • Key SOC challenges: alert fatigue, evolving threats, APTs, … **Week 2: Data Science/Engineering Foundations** *Summary:* Recap foundational concepts in data science and engineering with a focus on AI/ML.

	Lecture Content: • Data science/analytics concepts: statistical analysis. unsupervised and supervised ML, anomaly detection, neural networks, deep learning, reinforcement learning, CNN, RNNs, LSTM, … • Data engineering concepts: data cleaning, normalization, enrichment, ETL, distributed data processing and big data architectures., … **Week 3: Rise of AI – Generative Models & LLMs** *Summary:* Introduction to modern AI with a focus on generative models and LLMs. Bridge the gap between traditional data analytics and advanced AI concepts. *Lecture Content:* • Modern AI: Generative models and transformers. • LLMs and their architecture. *--Applications of AI in Cybersecurity--* ***Week 4: AI-powered Cyber Attack (Part 1)*** *Summary:* Explore how AI can be leveraged to automate and enhance cyber-attacks, guided by the MITRE ATT&CK framework. *Lecture Content:* • Introduction to cyber threat landscape: attackers TTPS • AI-powered social engineering and phishing attacks (initial access). • AI-generated malware (execution) ***Week 5: AI-powered Cyber Defense (Part 1)*** *Summary:* Explore how AI strengthens cyber defense and improves SOC operations, guided by NIST Cybersecurity framework.

	Lecture Content: • AI for advanced threat detection and hunting. • AI to enhance monitoring and reduce alert fatigue • AI for automated incident response ***Week 6: AI-powered Cyber Attack/Defense (Part 2) –*** *Flipped Classroom* *Summary:* A flipped classroom approach where students present on topics exploring AI applications in cyberattacks or defenses. Lecture Content: (Potential Topics) • AI-Driven Threat Intelligence • AI for Secure Coding • AI in Forensic Analysis and Incident Investigation • AI for Adoptive Honeypots and Sandboxes • AI-Powered Security Training and Awareness Programs • AI for Penetration Testing and Red Team Operations • AI for Vulnerability Management (Identification, Prioritization, and Patching) • AI for Reporting and Summarization • AI in Automated Reconnaissance • AI for Automated Exploit Generation • … ***Week 7: AI-powered Cyber Attack/Defense (Part 3)*** *Summary:* Continuing the lecture series on AI for defensive and offensive security. *Lecture Content:* • The missing topics from week 6. *--Concerns & Considerations of AI in Cybersecurity--* ***Week 8: Security Concerns in AI-driven Cybersecurity*** *Summary:* Addressing the security concerns and risks associated to AI systems and their usage in cybersecurity. *Lecture Content:* • AI-powered applications weaknesses & vulnerabilities. • Adversarial Machine Learning (weaknesses & vulnerabilities of AI models). • Related Frameworks: OWASP Machine Learning Security Top Ten, OWASP Top 10 for LLM Applications MITRE ATLAS, AIID, ADML.

	Week 9: Reliability in AI-driven Cybersecurity *Summary:* Focusing on key considerations when applying AI systems in cybersecurity. *Lecture Content:* • Importance of explainability and interpretability in AI (Explainable AI - XAI). • Building trust and ensuring accountability in AI-driven systems. • Domain-specific AI models (RAG systems) and the importance of fine-tuning. • Metrics and KPIs for benchmarking AI systems in cybersecurity (robustness, accuracy, security, etc.). ***Week 10: Responsible AI-driven Cybersecurity*** *Summary:* Examine the ethical, legal, and regulatory concerns associated with AI, particularly in cybersecurity. *Lecture Content:* • Ethical considerations of AI systems: fairness, bias, and transparency. • Privacy concerns with AI systems • Legal and regulatory requirements for AI systems, e.g., GDPR, AI Act, etc. *--Emerging Cross-cutting Topics—* ***Week 11: Future Trends in AI & Cybersecurity*** *Flipped classroom + (optional) guest lecture* *Summary:* Engage students (in form of flipped classroom) in exploring cutting-edge trends and controversial topics in AI and cybersecurity. Guest lecture (if available) to provide industry insight. *Lecture Content: (potential topics)* • Post-quantum cryptography and AI's role in post-quantum security • AI in zero trust architecture

	• Privacy-preserving AI & federated learning • AI and its impact on cyber warfare • AI in zero-day exploit discovery • AI at the edge (from cloud computing to edge computing) • Trust in the era of AI generated data • Human-AI Collaboration • AI-generated vulnerable codes ***Week 12: Wrap-up*** • *Overview of the course.* • *Final project presentations by students.* • *Discussions.* • *Guest lecture (from industry).*

Exams and assessment formats	• *Mid-term assessment (quiz) end of W5 (10%)*
	• *Flipped classroom in W6 & W11 (20%)*
	• *Group project from W6 to W12 (70%)*
	  o *Intermediate presentation (a pitch) in W8 (10%)*
	  o *Final presentation in W12 (30%)*
	  o *Technical report / scientific paper by W12 (30%)*

Study and examination requirements	*Students must have a 60% or higher final grade to pass.*
Reading list	***Recommended Reading Material:*** 1. *Muniz, Joseph. The modern security operations center. Addison-Wesley Professional, 2021. >>LINK<<* 2. *Abbas, R., Michael, K., Pitt, J., Vogel, K. M., & Zafeirakopoulos, M. (2023). Artificial Intelligence (AI) in Cybersecurity: A Socio-Technical Research Roadmap. The Alan Turing Institute. >> LINK <<* 3. *European Union Agency for Cybersecurity. (2022). Artificial intelligence and cybersecurity research. >> LINK <<* 4. *Sharma, R., Kalita, J., & Sharma, R. (2024). Artificial Intelligence in Cyber Security. ResearchGate. >> LINK <<* 5. *Kott, A. (2023). AI in Cybersecurity: The Paradox. IEEE Security & Privacy, 21(4), 94-98. >> LINK <<* 6. *Armando, A., Basile, C., Biondi, F., Botta, A., Carbone, R., Catania, V., Chessa, S., Ferretti, S., Marotta, A., & Mazzeo, G. (2024). AI in Cybersecurity: Activities of the CINI-AIIS Lab at University of Genoa. ITAL-IA 2024. >> LINK <<* 7. *Choo, K. K. R., Dehghantanha, A., & Parizi, R. M. (2023). Artificial Intelligence in Cyber Security. Pearson.* 8. *Sikos, L. F., Stumptner, M., Mayer, W., Howard, C., Voigt, S., & Philp, W. (2023). AI in Cybersecurity. 2023 Intermountain Engineering, Technology and Computing (IETC), 1-6. >> LINK <<*

	9. *Liu, Y., Zhao, X., & Sun, Y. (2023). Adversarial machine learning in cybersecurity: Challenges and opportunities. IEEE Transactions on Information Forensics and Security, 18, 2614-2629. >> LINK <<* 10. *Patel, A., & Johnson, M. (2024). Securing the Internet of Things: AI-driven approaches and challenges. IEEE Internet of Things Journal, 11(3), 1852-1867. >> LINK <<* 11. *Nguyen, T., & Anderson, K. (2023). Ethical considerations in AI-driven cybersecurity: A framework for responsible implementation. AI and Ethics, 3(4), 401-418. >> LINK <<*

Business Resilience, Threat Response, and Incident Management

Module designation	*Business Resilience, Threat Response, and Incident Management*
Semester(s) in which the module is taught	*Full Time* — *Semester 2 (Year 1)* *Part Time (Option I)* — *Semester 1 (Year 2)* *Part Time (Option II)* — *Semester 3 (Year 1)*
Person responsible for the module	*Michael Bradford < michael.bradford@ncirl.ie> (NCI)*
Language	*English*
Relation to curriculum	*Mandatory*
Teaching methods	*The teaching and learning strategy for the Business Resilience, Threat Response, and Incident Management module will consist of classes and directed activities such as videos, tutorials, case studies and discussions on the programme's Learning Management System (LMS). Each week learners will begin by engaging with 2 hours of directed online activities aimed at introducing threshold concepts for that week's topic. Directed activities consist of short digestible pieces of content, such as explanatory videos, reading, guided tutorials, etc. Learners will then attend a live 1-hour lecture and a 1-hour tutorial session. Learners will be assigned tasks and exercises related to the directed content so that they can connect the theory to practice. Live sessions will mostly be practically based so as to make best use of the lecturer's expertise in the classroom. Learners will benefit from mentoring and formative feedback on completed directed activities during classes.* *The learning and assessment materials will be made available to learners through the programme's LMS. To support learners' independent learning the lecture notes and lab materials will be complemented by links to additional resources available on the Internet (e.g., documentation/framework tools, tutorials/videos, etc.).*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 250 hours* *Directed e-Learning Activities: 24 hours* *Synchronous Lectures: 12 hours* *Tutorial Sessions: 12 hours* *Private study including examination preparation, specified in hours[1]: 202 hours*
Credit points	*10 ECTS*
Required and recommended prerequisites for joining the module	*N/A*

<table>
<tr><td>Module summary</td><td>This module aims to provide learners with knowledge on documentation, strategies, and technologies that support the processes of business resilience, threat response, and incident management. The module will examine how an organisation can prepare for business disruption and what actions can be taken to prevent and contain an incident, reduce the impact to organisational systems and get the business operational as quickly as possible after an incident occurs. Learners will acquire the necessary incident management skills required to develop contextual plans, run books and the associated processes and tools to enable effective business resilience capabilities. Furthermore, learners will be able to identify and illustrate the challenges associated with developing risk-based business resilience, threat response, and incident management processes. Learners will gain practical experience in aligning an organisation to industry standards and best practices that are commonly used for business resilience, threat response, and incident management tasks incorporating several stages, including preparation for incidents, detection and analysis of a security incident, containment, eradication, and full recovery, and post-incident analysis and learning.</td></tr>
<tr><td>Module objectives/intended learning outcomes</td><td>The Business Resilience, Threat Response, and Incident Management module is focussed on enabling learners to build, operate and critically assess an organisation's incident response capabilities and the resilience of their current critical processes and services, including the systems underpinning them. This module will appraise the key technical controls required in addition to the people and process elements required to build and operate a resilient organisation. In addition to evaluating the risk profile of an organisation, the module will enable learners to understand the requirements for directing operations during an incident with next gen-technology mind-set.

On successful completion of this module the learner will be able to:
LO1: Evaluate incident response plans, their effectiveness and their alignment to industry leading standards and appropriate incident response principles and methodologies.
LO2: Critically appraise response activities for incident management from initial compromise to recovery and make recommendations for improvement.
LO3: Contrast methods to assess the maturity of an organisation's incident response capabilities.
LO4: Evaluate mechanisms to leverage blue team and the red team capabilities during an incident and appraise appropriateness and prioritisation for specific incident response use cases.</td></tr>
<tr><td>Content</td><td>Business Resilience, Threat Response, and Incident Management is a 10 ECTS module delivered over 4 hours per week for 12 weeks. An indicative schedule of topics to be addressed each week is outlined below:
<table>
<tr><th></th><th>Lecture Topic</th><th>Detail</th></tr>
<tr><td>1</td><td>Introduction</td><td>A background on the industry leading best practices (Including NIST Cybersecurity</td></tr>
</table>
</td></tr>
</table>

			Framework for Incident Response). Understanding what risk means for an organisation and how an event ties into risk management processes. Providing an overview of where IR impacts governance, risk and compliance. Legal and regulatory compliance requirements for cyber incidents. Resilience standards (ISO 22301). Principles of incident management (ISO/IEC 27035).
	2	Assessing Impact of Cyber Attacks	Understanding the threat landscape, recent incidents and developments in IR tools and processes. Overview of business resilience with business continuity and the IR focus on availability, while managing disruption. Cloud platform considerations and challenges.
	3	System Security Concepts	How Blue teams evaluate and defend systems and environments. Understanding blue team activities during an incident.
	4	Scaling Incident Response	Shaping and improving your IR posture. Focus on Red teams and how they play the role of attackers by identifying security vulnerabilities and launching attacks within a controlled environment. Understanding when and how to use a red team during an incident.
	5	IR Roles and Responsibilities	Computer Incident Response Teams (CIRTs) operation. A mapping of IR roles to activities. How to prioritise these when directing incident response activities. Incident Management, Crisis Management and Business Continuity. Executive level stakeholders.
	6	Incident Response Process	IR activities and processes to gain Business input for IR. Incident Response Plan. Detection, Investigation, Analysis and Activation. Cross-domain and border-domain knowledge related to cybersecurity.
	7	Business Processes	The business perspective on regulation and operational resilience. Business Impact Analysis. The importance of process and service mapping to systems. Organisational and governance impact.
	8	System Forensics and Tools	The role of Incident Response, Forensics and E-discovery and the intersection. Focus on system forensics and tools from an IR perspective.

	9	Threat Intelligence & Threat Response	Threat intelligence processes. Importance of SIEM from threat hunting to performance monitoring.
	10	Security operations for IR	Secure Operation Centres (SOCs) operation. Approaches, processes and roles within Sec Ops for monitoring, the three-tiered model for SOC. Threat intelligence processes and tooling.
	11	IR Improvement process	How to evaluate your organisation's posture for IR. IR Reporting. IR Measurement. IR Auditing. IR Testing. Post incident activities supporting continuous improvement.
	12	Summary	Re-cap on core domains and takeaways.

Exams and assessment formats

The summative assessment strategy for this module is shown in the table below.

Assessment Type	*Assessment Description*	*Outcome addressed*	*%*	*Assessment Date*
Continuous Assessment 1	*For this assessment learners will have to evaluate real-world incidents and critique the incident response process. The CA is based on course content covered up to the date of assessment. Critical appraisal and evaluation required.*	*LO1, LO2, LO3*	*40*	*Week 5*
Continuous Assessment 2	*Terminal assessment based on 5 varied themes covered during the course requiring critical evaluation and demonstration of conceptual learning based on scenarios, research and critical appraisal.*	*LO1, LO2, LO3, LO4*	*60*	*Week 11*

Reassessment strategy:

The reassessment strategy for this module will consist of an assessment that will evaluate all learning outcomes.

Study and examination requirements

Learners must have an overall final grade of 40% or higher to pass this module.

Reading list

Recommended Book Reading

- *Anson, S. (2020). Applied Incident Response. 1st edition. John Wiley & Sons. [ISBN: 978-1119560265]*
- *Diogenes, Y., & Ozkaya, E. (2022). Cybersecurity–Attack and Defense Strategies: Improve your security posture to mitigate risks*

	and prevent attackers from infiltrating your system. 3rd Edition. Packt Publishing Ltd. [ISBN: 978-1803248776] • *Crask, J. (2024). Business Continuity Management: A Practical Guide to Organizational Resilience and ISO 22301. 2nd edition. Kogan Page [ISBN: 978-1398614871]* *Supplementary Book Reading* • *Thomas, A.E. (2018). Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence. [ISBN: 978-1643169705]* • *Thompson, E. C. (2018). Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents. 1st Edition. Apress. [ISBN: 978-1484238691]* • *Bautista, W. (2018), Practical Cyber Intelligence: How action-based intelligence can be an effective response to incidents [ISBN: 978-1788625562]* *Other Resources* **Description** / **URL** Verizon Breach Report — https://www.verizon.com/business/resources/reports/dbir/ Sans Reading Room — https://www.sans.org/reading-room/ Incident Handler's Handbook — https://www.sans.org/white-papers/33901/

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Cybersecurity Culture, Strategy & Leadership

Module designation	*Cybersecurity Culture, Strategy & Leadership* *(The CISO Fundamentals)*
Semester(s) in which the module is taught	*Winter*
Person responsible for the module	*Georges Ataya <ga@atayapartners.com> (Solvay Brussels)* *Evaldas Bruze <evaldas@l3ce.eu > (VMU, Kaunas)*
Language	*English*
Relation to curriculum	*Mandatory*
Teaching methods	Pre reading, Lectures, Case studies
Workload (incl. contact hours, self-study hours)	*Pre reading: (12 hours before and during the module delivery); Lectures (12*2 hours); Case study and workshop (6 hours over 12 weeks laps time in groups of students); module exam (2 hours in a multiple-Choice examination)*
Credit points	10
Required and recommended prerequisites for joining the module	No additional requirements specific for this module.
Module summary	Management practices for Chief Information Security officers and those reporting to this function include various management practices, involve specific culture and involves developing adequate strategy. This module addresses those management practices and train students on understanding and applying those practices. It includes implementing those processes and practices including the seven maturity components to ensure resilient operations.
Module objectives/intended learning outcomes	**Upon completion of this module, the learner will be able to gain a thorough understanding of the role of the CISO and key cultural and governance practices to achieve protection objectives. They will also develop the skills necessary to effectively exercise leadership responsibilities in planning, construction, operation and monitoring activities.** **Learning outcomes that students should attain in the module in terms of:** **LO1. Knowledge: Understanding of the role of the CISO and the culture and governance practices that are essential for reaching protection objectives. An understanding of Threats, vulnerabilities and overall protection controls that are required.**

	LO2. Skills: Possess the necessary skills to master the various CISO role in relation of completing leadership tasks in plan, build, run, and monitor domains of activities. **LO3. Competences: Students must be able to build a working CISO organisation and define relevant activities in line with business objectives.**
Content	1. ***The cybersecurity landscape including review of some narrated incidents. Overview of potential business impacts.*** 2. ***Overview of cybersecurity threats*** 3. ***Overview of cybersecurity vulnerabilities*** 4. ***Overview of controls as structured following major categorisations (four ISO 27001 domains, Five NIST domains, etc.)*** 5. ***Review of major cybersecurity related frameworks and regulations*** 6. ***The governance activities and the PLAN domains of governance.*** 7. ***Case Discussion: Building a CISO culture, a function and align with the organisation*** 8. ***The Risk Management process: Business and technology risks*** 9. ***The protection roadmap The BUILD domains of governance to implement relevant transformation actions*** 10. ***Incident management, CERT and the RUN domains of governance*** 11. ***The MONITOR domain including the seven components of maturity and the definition of security Dashboards (technical and managerial).*** 12. ***Understand the various cybersecurity roles and the development of a CISO organisation***
Exams and assessment formats	*One short computer-based quizzes after the sessions 5 and 10.* *One written assignment related to the development of a CISO organisation in a specific industry with specific technology and business requirements.*
Study and examination requirements	*Requirements for successfully passing the module* *e.g. the final grade in the module is composed of 60% performance on exams, 10% quizzes, 10% take-home assignments, 10% in-class participation. Students must have a final grade of 60% or higher to pass*
Reading list	*The virtual CISO article* *NIST CSF 2.0* *ENISA CSF* *CISM BOK (ISACA.org) - description videos*

	https://www.bing.com/ck/a?!&&p=cf68174b44ef6b6bJmltdHM9MTcyNTIzNTIwMCZpZ3VpZD0xYWUyY2FhNS03OTg5LTY1NjktMGQ0MS1kZTI4NzQ4ZjY0ZjcmaW5zaWQ9NTE1NQ&ptn=3&ver=2&hsh=3&fclid=1ae2caa5-7989-6569-0d41-de28788f64f7&u=a1L3ZpZGVvcy9zZWFyY2g_cT1jaXNtK2RvbWFpbnMmcXB2dD1jaXNtK2RvbWFpbnMmRk9STT1WRFJF&ntb=1 (PDF) Challenges and Solutions for Cybersecurity and Information Security Management in Organizations (researchgate.net) Challenges and Solutions for Cybersecurity and Information Security Management in Organizations March 2024 Vladimer Svanadze Sergiy Gnatyuk Cybersecurity and Strategic Management | Request PDF (researchgate.net) Cybersecurity and Strategic Management September 2023 DOI: 10.17323/2500-2597.2023.3.88.97 Budi Budi Gunawan Barito Mulyo Ratmono Ade Gafar Abdullah

Dissertation

Module designation	*Dissertation*
Module summary	After taking this module, you will have knowledge of research in your specialisation area. You will have an understanding of academic theory and the preparation of research pertinent to your field of study. You will be able to select appropriate research methods and techniques suitable for your research field You will understand the current state of the art in your research area, and be able to appropriately employ methods and existing research results in the development of new knowledge, theories and presentation of research in your research area
Semester(s) in which the module is taught	4 (assuming full-time)
Person responsible for the module	Jan Jürjens
Language	English
Relation to curriculum	Compulsory
Teaching methods	Dissertation
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload:* *Contact hours (please specify whether lecture, exercise, laboratory session, etc.): 18 (1-1 meetings)* *Private study including examination preparation, specified in hours[1]: 782*
Credit points	*25*
Required and recommended prerequisites for joining the module	Research methods
Module objectives/intended learning outcomes	The Dissertation should show that the candidate is able to familiarise him/herself with a scientific problem of the degree programme, solve it (if necessary with assistance by the supervisor) and write the result in an appropriate form. More specifically, the learning outcomes fall in the following categories: Knowledge The Knowledge learning outcomes are primarily achieved through the development of the dissertation and guidance provided by the supervisor during the course of the programme. The development of the thesis will generally arise as to ensure that the student is conversant with and in his or her area of

	specialisation at the research in their field. The outcomes of the individual research towards the dissertation will result in: Expected Knowledge Learning Outcomes 1. Knowledge of research in the candidate's specialisation area 2. Understanding of academic theory and the preparation of research pertinent to the field of study 3. Ability to select appropriate research methods and techniques suitable for the candidate's research field 4. Understanding the current state of the art in the individual research area, and the ability to appropriately employ methods and existing research results in the development of new knowledge, theories and presentation of research in the individual research area Skills The learning outcomes in the Skills domain relate to activities in the research community. The precise skills possible to acquire within the context of an individual study plan will vary as some research is intrinsically more collaborative in nature while other research may essentially be a largely solitary endeavour. Where appropriate, the programme will seek to impart skills suitable to the active participation in collaborative research and, on completion, also the ability to independently conduct research within an academic context. Successful completion of the programme enables to translate the understanding of processes and dynamics from observations and taught elements into such abilities. As in case of the previously described Knowledge outcomes, the preparation of the dissertation forms a significant part of the development of these learning outcomes. The experiences passed on from the supervisor to the student's ability to interact with the research community and to disseminate their research findings. The outcomes of the individual research will result in the following Expected Skills Learning Outcomes 1. Ability to perform the planning and preparation as well as to perform research projects in an academic setting 2. Ability to support and participate in academic research 3. Ability to comprehend academic issues and the related ethical considerations pertaining to the design and conduct of research 4. Ability to understand and challenge the existing knowledge and practise in the chosen specialisation area of Cyber Security
Content	The content depends on the individual dissertation.
Exams and assessment formats	Dissertation.

Study and examination requirements	Passing grade for the dissertation. The following aspects are taken into account for the grading: 1. Research topic and purpose 2. Knowledge of the research field and related theories as well as the use of literature 3. Material, acquisition of material and analyses (=methods) 4. Research results and reporting 5. Examination of results (discussion) and conclusions 6. Structure, clarity and polishing of the thesis 7. Conduct of the work during the thesis process
Reading list	The reading list depends on the individual dissertation.

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Internship

Module designation	*Internship*
Module summary	After taking this module, you will be able to analyse employer requirements and be able to articulate one's skills and experience related to these. You will be able to effectively demonstrate one's professional skills in a work environment. You will be able to critically reflect on the learning activities and experiences from the internship. You will be able to create an individual learning plan to identify meaningful personal and professional goals.
Semester(s) in which the module is taught	4 (assuming full-time)
Person responsible for the module	Jan Jürjens
Language	English
Relation to curriculum	Compulsory
Teaching methods	Internship report
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload:* *Contact hours (please specify whether lecture, exercise, laboratory session, etc.): 18 (1-1 meetings)* *Private study including examination preparation, specified in hours[1]: 782*
Credit points	*25*
Required and recommended prerequisites for joining the module	Research methods
Module objectives/intended learning outcomes	This module provides valuable work experience through an internship project which fits around the studies. Participants will be supported in choosing an internship across different organisations in the public, private, and charities sectors. Possible internships providers include local and national charities, small businesses, financial organisations, universities, political parties, museums, local councils, and schools. In this module, participants will:

	• be given the opportunity to do an internship during the semester while building transferable skills • learn how to relate key employability concepts directly to one's career journey • explore current developments in the graduate employability landscape By the end of the module participants will be able to: • analyse employer requirements and be able to articulate one's skills and experience related to these • effectively demonstrate one's professional skills in a work environment • critically reflect on the learning activities and experiences from the internship • create an individual learning plan to identify meaningful personal and professional goals
Content	The content depends on the individual internship.
Exams and assessment formats	Internship report.
Study and examination requirements	Passing grade for the internship report. The following aspects are taken into account for the grading: 1. Internship topic and purpose 2. Knowledge of the internship field 3. Material, acquisition of knowledge 4. Internship results and reporting 5. Examination of results (discussion) and conclusions 6. Structure, clarity and polishing of the internship report 7. Conduct of the work during the internship
Reading list	The reading list depends on the individual internship.

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Enterprise Architecture & Infrastructure Design (including Cloud)

Module designation	*Enterprise Architecture & Infrastructure Design (including Cloud)*
Semester(s) in which the module is taught	Year 1 Semester 1
Person responsible for the module	Gillian O'Carroll <> (MTU) Jacqueline Kehoe <> (MTU)
Language	English
Relation to curriculum	Compulsory
Teaching methods	Lectures & Independent Study
Workload (incl. contact hours, self-study hours)	Total workload: ***250 hours (60 Contact + 190 Independent Learning)*** Contact hours (please specify whether lecture, exercise, laboratory session, etc.): **Lectures: 12 x 2 hours = 24 hours** **Labs: 12 x 2 hours = 24 hours** **Tutorial: 12 x 1 hour = 12 hours** Private study including examination preparation, specified in hours[1]: **Independent Learning: 190 hours**
Credit points	**10 Credits**
Required and recommended prerequisites for joining the module	*N/A*
Module summary	Evaluate the importance of enterprise security architecture and infrastructure design to protect the organisation's systems and data from cybersecurity and other digital threats. Appraise the key computer network controls required to protect a network from various forms of attack. Analyse the security of cloud environments, identifying the critical similarities and differences between cloud and network security.
Module objectives/intended learning outcomes	**L01** Evaluate Enterprise Security Architecture and cybersecurity controls to achieve Defense in Depth (DiD) to protect the

	confidentiality, integrity, and availability of the data within an enterprise infrastructure **L02** Appraise various computer protection components such as Firewalls, VPN and Intrusion Detection and Response Systems (NIDRS) with the aim of protecting a network against various forms of attacks. **L03** Evaluate the applicability and use of Cybersecurity Architecture Frameworks to support secure systems in an enterprise infrastructure. **L04** Appraise cybersecurity controls and techniques in the design of an enterprise architecture to meet confidentiality, integrity and availability (CIA) requirements. **L05** Examine the foundational principles of cloud security, distinguishing it from traditional IT security and the nuances of various cloud architectures and service models **L06** Appraise the security of a cloud based virtualized architecture with the aim of protecting data, application and services.
Content	*The short description of the contents should clearly indicate focus areas and the level of difficulty.* ***Please divide the content into 12 sections (1 per week).*** **Week 1: Cyber Threats, Vulnerabilities and Attack Vectors** ENISA threat landscape i.e. malware, insider threats, web-based attacks, botnets, information leakage, cyber espionage, identity theft, ransomware, data breaches, denial of service, spam, phishing, crypto jacking. Structure of threat landscape. Threat actors, agents and trends – attack vectors, misinformation, disinformation, fileless and memory attacks, multi staged and modular threats etc. Threat intelligence and sharing. CIA Triad. Vulnerability types for wired and wireless networks. Vulnerability assessment. Penetration testing. Vulnerability database i.e. CVE Details.

	Week 2: Network Security Architecture Defense in Depth. Admin controls - policy and procedures. Technical Controls - network, hardware and software. Physical controls. Access measures. Workstation defense - anti spam. Data Protection. Perimeter Defense. Monitoring and Prevention. **Week 3: Security Principles – Firewalls & Zoning** Packet Filters (ACLs), Stateful, Stateless, Bastion Host, Circuit Level, Application Gateway, SOCKS, DMZ, Host-Based Firewall, Egress Filtering, Network Address Translation (NAT), Multihoming, IPTables/NetFilter, implementing NAT, Next-Generation Firewalls (NGFW). **Week 4: Intrusion Detection & Prevention** Types of IDSs, Deployment of IDS systems, inline, passive, taps, span ports, Network IDSs, Anomaly based Detection and Signature based Detection, Evasion Techniques, False Positives, NIDS implementation using e.g. Snort, Suricata. Data Loss Prevention. IDS and Malware detection. Skill in configuring and ultilizing network protection components i.e. IDS. **Week 5: Security Principles – Encryption & VPN** Encryption of static data. Symmetric encryption and Asymmetric. Trusted certificates. Key selection, lifecycle, management, key rotation techniques and concepts. Internet Key Exchange (IKE). ISAKMP/Oakley. IPSec, AH, Encapsulating Security Payload (ESP). Tunnel mode, Transport mode, Virtual Private Networks (VPNs), Remote access, SSH Tunneling, Cloud Security Issues. **Week 6: Frameworks for Enterprise Security Architecture** SABSA - Enterprise Security Architecture. Cross Boundary Enterprise Security Framework (CB ESM). Cybersecurity Operations Centre (CSOC). The Open Group Architecture Framework (TOGAF). Critical review and comparison of different frameworks **Week 7: Security Controls** Access control and authentication mechanisms. Permissions and the role of authentication in access controls. Authentication mechanisms. Cryptography basics and its various applications.

	Week 8: Product Security Architecture Designing software with security in mind. Where security controls fit into software design and development. Secure Software Development Lifecycle, including CICD pipelines. Privacy by Design. Protecting IP in software products. Managing third party and technology partner ecosystem risks. Chip-to-Cloud Security. Secure product support, OWASP Top 10, Web App Firewalls, Security of containers. **Week 9: Evolution of Cloud Security** Origins and rise of cloud platforms & responsibility shifts. Major cloud providers. Cloud architectures: Public, Private, and Hybrid. Cloud service models: IaaS, PaaS, and SaaS. Threat vectors specific to cloud environments. Importance of cloud security & distinction from traditional IT security. Strategic alignment of security controls with business objectives. Cloud security best practices. **Week 10: Cloud Computing** Security Architecture and Networking Technologies as they apply and are used in the Cloud. Policies, technologies and control to protect cloud resources. Data Centres, Virtualisation, Data Containers, Automation, Micro-segmentation. Cloud-based attacks (Cryptojacking, E-skimming, Unauthorised Access) and security mechanisms (Network, Cloud Instance, DevSecOps, Containerization, Applications, File Storage, Conformity and Governance). The need for security design implementation built-in at the beginning of the design process, so as to guarantee a stronger and less vulnerable system architecture. **Week 11: Cloud Network Security, Data Security, Database & Application Security** CIA triad, Zero trust. Data residency and sovereignty. Cloud storage security. Secure key and secret management. Database offerings, encryption types & methods, data masking, auditing, threat detection, best practices. Virtual Machines, serverless functions, containers, app hosting, API hosting, threat detection, best practices. Virtual networks, network topology, subnets, peering, firewalls, VPNs, DDoS, monitoring, Multi-Cloud & Hybrid Cloud security. **Week 12: Overview of Course Material, Class Discussion & Guest Lecture (optional)**

Exams and assessment formats	*e.g. two oral Midterm assessments (20 minutes each) and one final oral exam (40 minutes), short computer-based quizzes, take-home written assignments* **1. Short computer-based quiz (20% of Final Grade) in Week 5.** **2. Short computer-based quiz (20% of Final Grade) in Week 7.** **3. Project + Written Report + Final Oral Exam (15 minutes maximum) at Semester End.** **The final grade in the module is composed of 40% performance on MCQs and 60% on take-home assignments which includes an oral exam. Students must have a final grade of 60% or higher to pass,**
Study and examination requirements	*Requirements for successfully passing the module* *e.g. the final grade in the module is composed of 60% performance on exams, 10% quizzes, 10% take-home assignments, 10% in-class participation. Students must have a final grade of 60% or higher to pass*
Reading list	**Recommended Book Resources:** Neil Rerup and Milad Aslaner. (2018), Hands-On Cybersecurity for Architects : Plan and Design Robust Security Architectures, Packt Publishing, [ISBN: 9781788830263] C. P. Gupta and K. K. Goyal. (2020), Cybersecurity: A Self-Teaching Introduction, Mercury Learning & Information, [ISBN: 9781683924982] Aditya K. Sood. (2021), Empirical Cloud Security, Mercury Learning and Information, p.450, [ISBN: 978-1683926856]. **Supplementary Book Resources:** Yuri Diogenes and Erdal Ozkaya. (2018), Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics, Packt Publishing, [ISBN: 9781788475297]. Jeremy Faircloth. (2016), Penetration Tester's Open Source Toolkit, Syngress, [ISBN: 9780128021497]. Charles J. Brooks, Christopher Grow, Philip Craig, and Donald Short. Cybersecurity Essentials, Wiley, [ISBN: 9781119362395]. Eric Cole. (2009), Network Security Bible, 2nd. Wiley, [ISBN: 9780470502495]. Mihir. Shah. (2023), Cloud Native Software Security Handbook, Packt Publishing, p.372, [ISBN: 978-1837636983].

	Tim Mather, Subra Kumaraswamy,Shahed Latif. (2009), Cloud Security and Privacy, "O'Reilly Media, Inc.", p.338, [ISBN: 9781449379513].

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Law, Compliance, Governance, Policy, and Ethics

Module designation	*Law, Compliance, Governance, Policy, and Ethics*
Semester(s) in which the module is taught	*1st semester Second Year*
Person responsible for the module	*Susanna Pozzolo <susanna.pozzolo@unibs.it> (UNIBS)* *Giorgio Pedrazzi <giorgio.pedrazzi@unibs.it> (UNIBS)*
Language	*English*
Relation to curriculum	*Compulsory*
Teaching methods	*lesson, case studies.*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 250 hrs* *Contact hours: 40 hours e-learning, 20 hours asynch* *Private study including examination preparation, specified in hours[1]: 190 hours (170 self-reading / 20 hours exams preparation)*
Credit points	*10*
Required and recommended prerequisites for joining the module	*Basic understanding of cybersecurity principles, computer networks, and foundational knowledge of legal frameworks.*
Module summary	*The "Law, Compliance, Governance, Policy, and Ethics" module focuses on equipping students with an in-depth understanding of the legal, ethical, and governance frameworks that shape cybersecurity practices. It provides comprehensive insights into data protection laws, governance structures, and the intersection of legal and ethical standards in organizational cybersecurity strategies. Students will engage with real-world applications of laws such as the GDPR, NIS2, and the Cyber Resilience Act learning how to implement compliance measures and ethical practices in diverse cybersecurity environments. Through case studies, discussions, and practical exercises, students will develop the skills needed to craft and assess policies, promote ethical cybersecurity practices, and lead with integrity in professional settings.*
Module objectives/intended learning outcomes	*Upon successful completion of this module, students will be able to:* ***Analyze Legal and Ethical Frameworks**: Analyze and critically evaluate legal frameworks and ethical standards in cybersecurity, including the overlap and differences between cybersecurity, data protection, and privacy.* ***Interpret and Apply Cybersecurity Laws and Regulations**: Interpret and apply legal requirements to protect information assets, ensuring compliance with international regulations and internal governance tools such as policies or standards.*

	***Craft and Evaluate Policies**: Craft and assess policies that address ethical, legal, and practical aspects of cybersecurity operations while promoting organizational integrity.* ***Integrate Ethical Cybersecurity Practices**: Integrate and promote ethical considerations in decision-making and conduct across all levels of the organization, enhancing organizational integrity through privacy, confidentiality, and accountability.* ***Champion Diversity and Inclusion**: Create and implement diversity and inclusion strategies within cybersecurity roles and policies to foster innovation, resilience, and organizational effectiveness.* ***Communicate Complex Concepts:** Communicate complex legal, ethical, and policy issues to diverse stakeholders to facilitate informed decision-making and ensure compliance.*
Content	***Week 1: Legal Foundations of Cybersecurity*** *An introduction to key legal instruments, foundational concepts, and essential terminology in cybersecurity law.* ***Week 2: Regulatory and Legal Aspects of Cybersecurity Strategy and Operations (I)*** *An overview of relevant laws, acts, and regulations at the EU level, including NIS2, DORA, and the Cyber Resilience Act.* ***Week 3: Regulatory and Legal Aspects of Cybersecurity Strategy and Operations (II)*** *Examination of the European regulatory landscape for the Digital Decade, with a focus on cybersecurity-related laws such as the AI Act, Data Act, DSA, and DMA.* ***Week 4: Data Protection and Privacy*** *In-depth analysis of GDPR principles, key concepts, and the roles and responsibilities of various stakeholders.* ***Week 5: Cross-Border Data Protection*** *Exploration of the Law Enforcement Directive, ePrivacy Directive, and regulations governing cookies, as well as issues surrounding international data flows.* ***Week 6: Accountability and Compliance Management*** *Discussion of accountability mechanisms and compliance management strategies within organizations, with a focus on specific sectors.* ***Week 7: Legal Frameworks and Compliance***

	A detailed study of how legislation underpins cybersecurity and data protection, emphasizing EU laws and corporate compliance mechanisms. ***Week 8: Standards and Certifications*** *Analysis of prominent EU cybersecurity standards and certifications, their enforceability, and the consequences of non-compliance.* ***Week 9: Governance in Cybersecurity*** *Examination of the integration of cybersecurity within broader IT governance frameworks and the role of policies in shaping organizational strategies.* ***Week 10: Ethical Considerations and Policy-Making*** *Exploration of the ethical dimensions of cybersecurity decisions and policy-making, with attention to the impact of emerging technologies like AI.* ***Week 11: Workplace Surveillance and Cybersecurity*** *A study of the balance between surveillance for security monitoring and the protection of employee privacy, analyzing surveillance technologies, legal frameworks, and ethical considerations to inform policy development.* ***Week 12: Diversity and Inclusion in Cybersecurity*** *Evaluation of the role of inclusive practices in enhancing cybersecurity efforts, and the impact of cyber-attacks on personnel, including psychological effects on response teams.*
Exams and assessment formats	Option 1: **Final Written Exam (Multiple-Choice Questionnaire)** – 30 minutes. This exam will cover key concepts, legal frameworks, and technical aspects of cybersecurity. Option 2: **Case Study Analysis or Presentation** – Students may alternatively choose to select a relevant case study related to workplace surveillance, cybersecurity strategy, or data protection laws. They will submit a detailed written analysis or deliver a presentation, demonstrating their ability to apply theoretical knowledge to practical scenarios.
Study and examination requirements	*Option 1:* *Final Written Exam (Multiple-Choice Questionnaire) – 50%* *Participation in Class Discussions and Activities – 30%* *Short Research Assignments or Quizzes – 20%* *Option 2:* *Case Study Analysis or Presentation – 50%*

	Participation in Class Discussions and Activities – 30% *Short Research Assignments or Quizzes – 20%* *Students must have a final grade of 60% or higher to pass*
Reading list	Understanding Cybersecurity Law in Data Sovereignty and Digital Governance An Overview from a Legal Perspective [2022] Melissa Lukings , Arash Habibi Lashkari https://link.springer.com/book/10.1007/978-3-031-14264-2 Handbook on European data protection law [2018] https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition# Guide to the General Data Protection Regulation (GDPR) https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Research Methods

Module designation	**Research Methods**
Semester(s) in which the module is taught	*1*
Person responsible for the module	Jan Jürjens
Language	English
Relation to curriculum	Mandatory
Teaching methods	The teaching and learning strategy for the Research Methods module will consist of classes and directed activities such as videos, tutorials, case studies and discussions on the programme's Learning Management System (LMS). Each week learners will begin by engaging with 2 hours of directed online activities aimed at introducing threshold concepts for that week's topic. Directed activities consist of short digestible pieces of content, such as explanatory videos, reading, guided tutorials, etc. Learners will then attend a live 2-hour discussion and tutorial session. Learners will be assigned tasks and exercises related to the directed content so that they can connect the theory to practice. Live sessions will mostly be practically based so as to make best use of the lecturer's expertise in the classroom. Learners will benefit from mentoring and formative feedback on completed directed activities during classes. The learning and assessment materials will be made available to learners through the programme's LMS. To support learners' independent learning the lecture notes and lab materials will be complemented by links to additional resources available on the Internet (e.g., documentation/framework tools, tutorials/videos, etc.).
Workload (incl. contact hours, self-study hours)	(Estimated) Total workload: 125 hours Directed e-Learning Activities: 12 hours Synchronous Tutorial Sessions: 12 hours Private study including examination preparation: 101 hours
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*N/A*
Module summary	After taking this module, you will be able to fully understand the range of research approaches, methodologies and strategies used in research within Cyber Security. You will have the tools and knowledge by which you can design a research proposal in Cyber Security applying relevant research strategies to collect and test data.

	You will know the evaluation methods in Cyber Security for qualitative and quantitative data. You are able to carry out appropriate research in Cyber Security ensuring an ethical research methodology is employed.
Module objectives/intended learning outcomes	LOs (according to Bloom's taxonomy): On successful completion of this module the learner will be able to: • LO1 (Knowledge): know the range of research approaches, methodologies and strategies used in research within Cyber Security • LO2 (Comprehension): comprehend the tools or knowledge by which they can design a research proposal in Cyber Security applying relevant research strategies to collect and test data; • LO3 (Application): apply evaluation methods in Cyber Security for qualitative and quantitative data; • LO4 (Analysis): carry out appropriate research analysis in Cyber Security ensuring an ethical research methodology is employed; • LO5 (Synthesis): develop capacity for analysis and synthesis of data instances in Cyber Security • LO6 (Evaluation): develop research skills on exploring real-world issues in Cyber Security
Content	**Module content** 1. **Introduction to Research** 2. **Theoretical foundations of Research Methods; Ethical Concerns (including wrt. the use of Generative AI)** 3. **Qualitative Research Methods** 4. **Quantitative Research Methods** 5. **Other Research Methods, in particular use of Generative AI** 6. **Different Research strategies** 7. **Research Design and Process** 8. **Data Collection Techniques** 9. **Interview Design and Analysis** 10. **Statistical Data Analysis (incl. Statistical tests)** 11. **Research Data Presentation** *12.* **Cyber Security Miniproject Presentations**
Exams and assessment formats	Cyber Security Miniproject presentation
Study and examination requirements	Requirements for successfully passing the module The final grade in the module consists of the miniproject grade.
Reading list	• Creswell, J. W. (2022**). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches**. 6th ed. Thousand Oaks, SAGE Publications: California.

	• Tang, H. (2020). **Engineering Research: Design, Methods, and Publication**. London: Wiley. ISBN: 978-1-119-62453-0 • Sönke Ahrens: **How To Take Smart Notes**, 2017 • Schmidt, J. F. K. (2016). **Niklas Luhmann's Card Index: Thinking Tool, Communication Partner, Publication Machine**. In A. Cevolini (Ed.), Forgetting Machines: Knowledge Management Evolution in Early Modern Europe (pp. 289-311). Brill. • Forte, T. (2022). **Building a Second Brain: A Proven Method to Organize Your Digital Life and Unlock Your Creative Potential**. Atria Books.

Security Operations

Offered by: CY Cergy Paris University

Credits: 10 ECTS (250 Student Work Hours)

The Security Operations module at CY Cergy Paris University is a comprehensive course designed to equip students with the essential knowledge and practical skills required for a career as a cybersecurity analyst within a Security Operations Center (SOC). This course, which carries a weight of 10 ECTS credits, corresponds to approximately 250 hours of total student effort. These hours are distributed between direct contact hours, including lectures and practical sessions, and self-study hours. The course provides a balanced approach that ensures both theoretical understanding and hands-on experience in cybersecurity operations.

Course Overview

The Security Operations module is tailored for students aspiring to develop a career in cybersecurity, specifically within SOCs. The course focuses on the fundamental principles of cybersecurity operations, network infrastructure vulnerabilities, and TCP/IP protocol suite operations. It covers a broad range of topics essential for understanding and managing cybersecurity threats in real-world environments.

Upon completion of this course, students will have the foundational knowledge necessary to assume the role of an entry-level cybersecurity analyst in a threat-focused SOC, with the capability to strengthen network protocols, secure devices, and enhance operational efficiency.

Course Structure and Content

The course is divided into multiple comprehensive sections, each focusing on a critical aspect of cybersecurity operations:

1. **Introduction to Security Operations Centers (SOC)** ○ Definition and role of a SOC within an organization's cybersecurity strategy.
   - Understanding the key functions and responsibilities of a SOC analyst.
   - Overview of SOC tools and technologies.
2. **Network Infrastructure and Security Monitoring Tools** ○ Understanding the architecture of network infrastructure.
   - Exploration of network monitoring tools and their applications in security. ○ Identification of network vulnerabilities and implementation of security measures.
3. **Data Categories and Analysis** ○ Overview of various data types used in security operations.
   - Techniques for collecting, categorizing, and analyzing security data.
   - Use of data to investigate and respond to security incidents.
4. **Fundamentals of Cryptography** ○ Basic concepts of cryptography and its role in cybersecurity.
   - Exploration of cryptographic technologies and protocols.
   - Application of cryptography in securing data transmission and storage.
5. **Common TCP/IP Attacks and Mitigation Techniques** ○ Understanding of common TCP/IP vulnerabilities. ○ Exploration of various TCP/IP-based attacks, such as SYN floods, IP spoofing, and DNS attacks.
   - Strategies for detecting and mitigating these attacks.
6. **Endpoint Security Technologies** ○ Introduction to endpoint security and its importance in a SOC. ○ Exploration of various endpoint security tools and

technologies. ○ Techniques for monitoring and securing endpoints against potential threats.
    - Hands-on experience with key SOC tools such as firewalls, intrusion prevention systems (IPS), and endpoint detection and response (EDR) solutions.
    - Configuration and management of SOC technologies.
7. **Incident Analysis in a Threat-Centric SOC** ○ Understanding the lifecycle of a security incident.
    - Techniques for analyzing and responding to security incidents in a SOC.
    - Use of threat intelligence in enhancing SOC capabilities.
8. **Cyber Threat Hunting and Intelligence Gathering** ○ Introduction to cyber threat hunting techniques. ○ Identification and use of resources for effective threat hunting.
    - Techniques for gathering and analyzing threat intelligence.
9. **Event Correlation and Normalization** ○ Understanding event correlation and its importance in security monitoring. ○ Techniques for normalizing and correlating security events.
    - Tools and methodologies for effective event correlation.
10. **Investigation of Security Incidents** ○ Detailed exploration of incident investigation processes. ○ Techniques for investigating and responding to various types of security incidents.
    - Use of security information and event management (SIEM) systems in incident investigation.
11. **SOC Workflow and Automation** ○ Overview of SOC workflows and processes.
    - Introduction to SOC automation tools and techniques.
    - Strategies for optimizing SOC workflows for improved efficiency.
12. **Incident Response and Management** ○ Understanding the principles of incident response. ○ Exploration of incident response methodologies and frameworks.
    - Techniques for managing and mitigating security incidents.
13. **Introduction to VERIS (Vocabulary for Event Recording and Incident Sharing)** ○ Overview of the VERIS framework and its application in cybersecurity.
    - Techniques for using VERIS to record and share incident data.
14. **Operating System Fundamentals: Windows and Linux** ○ Introduction to the Windows and Linux operating systems. ○ Exploration of OS-specific security features and vulnerabilities.
    - Techniques for securing and monitoring Windows and Linux systems.
15. **Advanced Topics in Cybersecurity:**
    - Threat hunting techniques.
    - Malware analysis and reverse engineering.
    - Automation and scripting in SOC environments.
16. **Legal, Ethical, and Compliance Issues in Cybersecurity:**
    - Understanding GDPR, HIPAA, and other relevant regulations. ○ Ethical considerations in cybersecurity operations.

Practical Exercises

The practical component of the course allows students to apply the knowledge gained through lectures to real-world scenarios. The hands-on labs are designed to simulate a variety of security operations tasks and incident response activities, including:

- Configuring and managing a collaborative lab environment.
- Using network security monitoring (NSM) tools to analyze data categories.

- Exploring cryptographic technologies and implementing them in a lab environment.
- Simulating and defending against TCP/IP attacks.
- Investigating hacker methodologies and identifying malicious activities.
- Hunting for cyber threats using advanced threat detection tools.
- Correlating event logs, packet captures (PCAPs), and alerts to analyze security incidents.
- Conducting detailed investigations into browser-based attacks and advanced persistent threats (APTs).
- Utilizing SOC playbooks for organized security monitoring and incident response.
- Conducting forensic analysis on Windows and Linux operating systems.

Learning Outcomes

By the end of the course, students will be able to: • Understand the role and operations of a SOC and its analysts.

- Utilize various network monitoring tools and techniques to detect and respond to security incidents.
- Analyze and interpret security data to identify potential threats and vulnerabilities.
- Apply cryptographic methods to secure data in transit and at rest.
- Investigate and respond to security incidents using established frameworks and methodologies.
- Develop and implement SOC workflows and automation strategies for improved operational efficiency.

Course Hours Distribution

- **Contact Hours (Lectures, Tutorials, Practical Sessions):** 100 hours
- **Self-Study Hours (Reading, Assignments, Exam Preparation):** 150 hours

The course provides a balanced blend of theoretical learning and practical application, ensuring that students are well-prepared for a career in cybersecurity. The practical sessions are integral to the course, allowing students to gain hands-on experience in managing and mitigating real-world cyber threats.

The total workload for the module is 250 hours, equivalent to 10 ECTS credits. The distribution of these hours is as follows:

- **Contact Hours (Lectures, Tutorials, Practical Sessions): 100 hours**

These contact hours are divided among various learning activities to enhance students' understanding and practical skills:

  - **Lectures:** 40 hours
    Lectures will cover the theoretical aspects of security operations, including key concepts, methodologies, and best practices. These sessions provide students with a foundation in cybersecurity principles and the functioning of a Security Operations Center (SOC).

  - **Tutorials:** 20 hours
    Tutorials are interactive sessions designed to reinforce the material covered in lectures. They provide an opportunity for students to engage in discussions, ask questions, and solve problems related to cybersecurity scenarios and SOC operations.

  - **Practical Sessions (Labs):** 40 hours
    Practical sessions offer hands-on experience with cybersecurity tools and technologies used in SOC environments. These labs focus on skills such as

configuring and using SIEM (Security Information and Event Management) systems, conducting threat analysis, and implementing incident response procedures.

- **Self-Study Hours (Reading, Assignments, Exam Preparation): 150 hours** Self-study hours are intended to deepen students' knowledge and understanding of the course material through independent learning activities:
  - **Reading:** 40 hours
    Students are expected to dedicate time to reading academic papers, textbooks, and other relevant materials that provide further insights into cybersecurity operations, threat intelligence, and incident response strategies.
  - **Assignments and Projects:** 60 hours
    Assignments and projects are important components of the course, allowing students to apply their knowledge to real-world scenarios. These tasks are designed to enhance critical thinking and problem-solving skills, as well as to encourage independent research and practical application of the concepts learned in class.
  - **Exam Preparation:** 50 hours
    Students should allocate time for exam preparation, including reviewing lecture notes, revisiting key topics, and practicing problem-solving for potential exam questions.

Prerequisites

Basic understanding of networking and operating systems is recommended. No prior experience in cybersecurity is required. To ensure that students are adequately prepared for the "Security Operations" module, the following prerequisites are recommended:

Basic Knowledge of Computer Networks: Students should have a foundational understanding of computer networking concepts, including TCP/IP, network protocols, and basic network security principles. This knowledge is essential for understanding how threats move through networks and how to implement effective monitoring and defense strategies.

Familiarity with Operating Systems: A working knowledge of both Windows and Linux operating systems is required. This includes understanding system architecture, file systems, user and group management, and command-line proficiency. Knowledge of operating systems is important for understanding how to detect and respond to threats on different platforms.

Programming and Scripting Basics**:** Basic programming and scripting skills, particularly in languages such as Python, Bash, or PowerShell, are advantageous. These skills are useful for automating tasks, developing custom tools, and conducting incident response activities within a SOC environment.

Basic Knowledge of Information Technology (IT) Infrastructure: Understanding the components and architecture of IT infrastructure, including servers, databases, cloud environments, and network devices, is beneficial. This knowledge helps students comprehend the operational context of SOC activities and the potential attack surfaces.

Assessment Methods

Assessments will include quizzes and tests, practical lab exercises, assignments and projects, and a final exam.

Technological Foundations in Computer Science and Security Controls

Module designation	*Technological Foundations in Computer Science and Security Controls*
Semester(s) in which the module is taught	*Mandatory course*
Person responsible for the module	*Răzvan Deaconescu (razvan.deaconescu@upb.ro) (UNSTPB)*
Language	*English*
Relation to curriculum	*Mandatory*
Teaching methods	*Lecture, lab*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 228* *Contact hours:* • *Lecture (a lot of demos): 48 hours,* • *Practice / laboratory session: 48 hours* o *Preset environments (local or remote virtual machines* *Private study including examination preparation, specified in hours[1]: 96 hours - used for preparing for sessions, solving assignments, preparing for examination, self-study* *Team project: 36 hours*
Credit points	*10*
Required and recommended prerequisites for joining the module	*Basic programming skills and knowledge: functions, structures, classes, recursion, programmer's toolchain* *Basic understanding and use of computing systems* *Comfort in using common applications in computing systems: web browsers, file browsers, Office suite, management of media files, email clients*
Module summary	*The "Technological Foundations in Computer Science and Security Controls" aims to create the fundamental set of skills and knowledge in computing systems and security. Students will gain understanding and competences expected for a system power user: investigate, update, configure, assess, monitor a computing system and its components, with particular focus on security.*
Module objectives/intended learning outcomes	*On successful completion of this module the learner will be able to:* *LO1: Outline the hardware-software stack in modern computer systems* *LO2: Define and explain fundamental security concepts* *LO3: Use applications to configure, secure, troubleshoot issues with data, applications and networking* *LO4: Develop basic programs using Python*

	L05: Examine, evaluate and revise security properties of data and applications: confidentiality, integrity, reliability *LO6: Identity and employ fundamental security requirements in existing applications and setups*
Content	1. *Computer Systems: Hardware, Software, Users* a. *Overview of computing systems, models* b. *Hardware, computer system types* c. *Software, applications the software stack* d. *(Security) Issues with computer systems* e. *Investigate the software and hardware information of a computing system* f. *Install and uninstall new applications* 2. *Tools and Common Applications of Computer Systems* a. *Applications and application types (for different system types)* b. *Local and web apps* c. *Using, configuring and customizing common applications* d. *Online and offline office suite software* e. *Synchronizing local, online and mobile apps and data* 3. *Data and Files* a. *Data storage and representation: bits, bytes, ASCII, UTF-8, binary, text* b. *Files and filesystems* c. *Working with data* d. *Finding data and files* e. *Best practices in organizing data* 4. *File Management and Access Control* a. *Users and access* b. *Filesystem permissions and access control* c. *Configuring filesystem permissions* d. *Fixing access control configuration issues* 5. *Storing and Versioning Data* a. *Requirements for versioning and history* b. *Versioning and history in common applications (Office Suites, storing applications)* c. *Backing up data* d. *Multi-versioning, version control systems* 6. *Data Processing and Visualisation* a. *Processing data, results of processing* b. *Viewing data, types of plots* c. *Visualization software* 7. *Secure Programming* a. *Common code weaknesses and vulnerabilities* b. *Best practices in programming* c. *Secure coding guidelines* d. *Secure coding in different programming languages* e. *Defensive programming* 8. *Secure Code Operations* a. *Secure Software Development Lifecycle* b. *Code Auditing* c. *Static and Dynamic Analys*

	d. *Software supply chain: building, packaging, delivery* e. *Continuous Integration & Continuous Delivery* 9. *Networking and Connected Systems* a. *Networking Concepts: Addressing, Communcation Media, Protocols* b. *Network Parameters and Configuration (addressing, gateway, DNS)* c. *Network applications and services* d. *Basic network troubleshooting* 10. *Fundamental Security Topics* a. *Security principles and concepts: threat model, subject-object model, access control, reference monitor, bug / vulnerability / exploits* b. *Security goals: integrity, confidentiality, reliability, availability, privacy* c. *Security in modern computer systems* d. *Data security, network security, web security, application security* 11. *Integrity and Confidentiality* a. *Requirements for integrity and confidentiality* b. *Encryption, encryption algorithms and tools* c. *Digital certificates, TLS, connection security* d. *Validating integrity and confidentiality* 12. *Authentication, Authorization and Access Control* a. *Authentication: Passwords, tokens, user IDs, two-factor* b. *Password best practices, password management, password leaks* c. *Authorization, permissions, roles* d. *Access control, ACLs* e. *Authentication, Authorization and Access Control databases* f. *A, A, AC in modern systems*
Exams and assessment formats	*Assignments (20%)* - *Practice exercises working with applications and files – 10%* - *Practice exercises on a networked system – 10%* *Team Project (30%)* - *Set up a (set of) secure, functional virtual machine(s) – 30%* *Final exam (40%)* - *Quiz (multiple answer questions) - 45 minutes: 20%* - *Practical exam: - 120 minutes: 20%*
Study and examination requirements	*The final grade in the module is composed of 40% performance on exams, 50% take-home assignments and project, 10% in-class participation. Students must have a final grade of 50% or higher to pass*
Reading list	*Computer Systems: A Programmer's Perspective, 3rd Edition (https://csapp.cs.cmu.edu/)* *The Missing Semester of Your CS Education (https://missing.csail.mit.edu/)* *Security Essentials: https://github.com/open-education-hub/essentials-security* *Common Weakness Enumeration: https://cwe.mitre.org/* *SEI CERT Coding Standards: https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards*

Automation of Security Tasks and Data Analytics

Module designation	*Automation of Security Tasks and Data Analytics*
Semester(s) in which the module is taught	*2nd or 3rd*
Person responsible for the module	*Prof. Sanda Martinčić-Ipšić, PhD <smarti@uniri.hr> (UNIRI)* *Prof. Marina Ivašić-Kos, PhD <marinai@uniri.hr> (UNIRI)*
Language	*English*
Relation to curriculum	*Elective* *Cyber Threat Intelligence Specialist*
Teaching methods	*Lesson, lab works, project*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload:* ***150 hours*** *Contact hours:* ***Synchronous Lectures: 12 hours*** ***Tutorial Sessions: 12 hours*** ***Directed e-Learning Activities: 24 hours*** ***Independent learning and work on project: 102 hours***
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*None*
Module summary	This course provides a comprehensive introduction to using Python for automating cybersecurity tasks, including threat detection, intelligence gathering, vulnerability assessment, and incident response. Students will learn to write scripts, analyze data and integrate various tools, while adhering to ethical and legal guidelines in cybersecurity automation.
Module objectives/intended learning outcomes	On successful completion of this module the learner will be able to: *LO1: Utilize Python to implement advanced cybersecurity tasks, including configuring environments, writing scripts for network scanning, log analysis, vulnerability assessment, and ensuring secure coding practices..* *LO2: Design and implement automated processes for threat detection, threat intelligence gathering, and incident response using Python, integrating various cybersecurity tools.* *LO3: Use Python to manipulate, analyze, and visualize data related to cybersecurity, enhancing threat intelligence through data analysis.*

	LO4: Apply ethical and legal standards in the automation of cybersecurity tasks, including web scraping and threat intelligence gathering, ensuring compliance with industry regulations and ethical principles. *LO5: Independently create and refine automated solutions for cybersecurity challenges and communicate the importance and impact of automation in cybersecurity.*

Content	**12-Week Program: Automation of Security Tasks**
	Week 1: Introduction to Python and Cybersecurity
	• **Classes:**
	  ○ Focus Areas: Introduction to Python programming language, Overview of Python in cybersecurity, Basic programming concepts.
	  ○ Level of Difficulty: Introductory
	• **Labs:**
	  ○ Focus Areas: Setting up Python environment, Writing and running basic Python scripts using Jupyter Notebook and/or Anaconda.
	  ○ Level of Difficulty: Introductory
	Week 2: Automating Reconnaissance
	• **Classes:**
	  ○ Focus Areas: Reconnaissance techniques in cybersecurity, Importance of reconnaissance in cyber threat intelligence, Tools and methods for reconnaissance.
	  ○ Level of Difficulty: Introductory to Intermediate
	• **Labs:**
	  ○ Focus Areas: Writing Python scripts to perform active scanning and search open technical databases using libraries for network interaction such as `scapy` and HTTP requests with `requests`.
	  ○ Level of Difficulty: Introductory to Intermediate
	Week 3: Threat Intelligence Fundamentals
	• **Classes:**
	  ○ Focus Areas: Introduction to threat intelligence, Sources of threat intelligence,

	Types of threat intelligence (strategic, operational, tactical, technical). o Level of Difficulty: Intermediate • **Labs:** o Focus Areas: Gathering threat intelligence using Python from OSINT feeds, social media, and forums using parsing tools such as `BeautifulSoup` and HTTP requests with `requests` o Level of Difficulty: Intermediate **Week 4: Data Analysis and Visualization for Threat Intelligence** • **Classes:** o Focus Areas: Importance of data analysis in threat intelligence, Techniques for data cleaning, transformation, and visualization. o Level of Difficulty: Intermediate • **Labs:** o Focus Areas: Using Python libraries such as `Pandas` for data manipulation and `Matplotlib` for visualization of threat intelligence data o Level of Difficulty: Intermediate **Week 5: Automating Log Analysis and Monitoring** • **Classes:** o Focus Areas: Importance of log analysis in cybersecurity, Techniques for parsing and analyzing log files. o Level of Difficulty: Intermediate • **Labs:** o Focus Areas: Writing Python scripts to automate log analysis and monitoring using logging libraries such as the built-in `logging` module and `Loguru`. o Level of Difficulty: Intermediate **Week 6: Network Traffic Analysis** • **Classes:** o Focus Areas: Introduction to network traffic analysis, Importance in threat intelligence, Tools and techniques for analyzing network traffic.

	○ Level of Difficulty: Intermediate to Advanced • **Labs:** ○ Focus Areas: Writing Python scripts to capture and analyze network traffic using libraries for network analysis such as `scapy`. ○ Level of Difficulty: Intermediate to Advanced **Week 7: Incident Detection and Response Automation** • **Classes:** ○ Focus Areas: Incident detection and response processes in threat intelligence, Automating detection of suspicious activities, Tools for incident response automation. ○ Level of Difficulty: Intermediate to Advanced • **Labs:** ○ Focus Areas: Developing Python scripts to automate incident detection and response workflows using system monitoring libraries such as `psutil` for system resource monitoring and `subprocess` for executing system commands ○ Level of Difficulty: Intermediate to Advanced **Week 8: Threat Hunting Automation** • **Classes:** ○ Focus Areas: Introduction to threat hunting, Techniques and tools for threat hunting, Automating threat hunting tasks. ○ Level of Difficulty: Advanced • **Labs:** ○ Focus Areas: Writing Python scripts to automate threat hunting activities using threat intelligence data and query libraries such as `elasticsearch` . ○ Level of Difficulty: Advanced **Week 9: Vulnerability Management and Exploitation** • **Classes:**

	○ Focus Areas: Common vulnerabilities and exploitation methods, Automating vulnerability assessments. ○ Level of Difficulty: Intermediate to Advanced • **Labs:** ○ Focus Areas: Conducting automated vulnerability assessments and exploiting vulnerabilities using Python and tools for vulnerability scanning and exploitation such as `nmap` and `metasploit`. ○ Level of Difficulty: Intermediate to Advanced **Week 10: Advanced Web Scraping for Threat Intelligence** • **Classes:** ○ Focus Areas: Advanced techniques for web scraping, Legal and ethical considerations in web scraping. ○ Level of Difficulty: Intermediate to Advanced • **Labs:** ○ Focus Areas: Writing Python scripts for advanced web scraping and data extraction using web scraping tools such as `BeautifulSoup`, `Scrapy`, and browser automation tools such as `Selenium`. ○ Level of Difficulty: Intermediate to Advanced **Week 11: Automating AI Models for Threat Intelligence** • **Classes:** ○ Focus Areas: Introduction to AI in cybersecurity, Using pre-trained AI models for threat intelligence, Methods for integrating AI into threat intelligence workflows. ○ Level of Difficulty: Advanced • **Labs:** ○ Focus Areas: Writing Python scripts to forward data to free AI models (e.g.,

	OpenAI, Hugging Face) and processing responses for threat intelligence. ○ Level of Difficulty: Advanced **Week 12: Integrating and Automating Security Tools** • **Classes:** ○ Focus Areas: Integration of various security tools, Building automated workflows, Best practices for automation in security. ○ Level of Difficulty: Advanced • **Labs:** ○ Focus Areas: Creating and deploying integrated automation solutions for security tasks using Python and orchestration tools such as `Docker` and `Ansible`. ○ Level of Difficulty: Advanced
Exams and assessment formats	*Midterm assessment, take-home lab assignments*
Study and examination requirements	*2 Midterm assessment (online quiz 25 minutes each)* *Project assignments on selected topics with documentation and oral presentation* *The final grade in the module is composed of 50% performance on two midterms (50% needed to pass), 50% project assignment (30% practical work, 10% oral presentation, 10% technical documentation).* *Students must have a final grade of 60% or higher to pass*
Reading list	Mandatory Reading: • Poston III, H. E. (2022). Python for Cybersecurity: Using Python for Cyber Offense and Defense. Wiley. ISBN: 978-1-119-85064-9 • Python Documentation. Available at: https://docs.python.org/ • Pandas Documentation. Available at: https://pandas.pydata.org/pandas-docs/stable/ • MITRE ATT&CK Framework. Available at: https://attack.mitre.org/

	Elective Reading (For Deeper Understanding and Additional Practice): • Sweigart, A. (2019). Automate the Boring Stuff with Python: Practical Programming for Total Beginners (2nd ed.). No Starch Press. ISBN: 978-1-59327-992-9. • Bautista Jr., W. (2018). Practical Cyber Intelligence: How Action-Based Intelligence Can Be an Effective Response to Incidents. Packt Publishing. ISBN: 978-1-78862-556-2

CISO and Crisis Communication

Module designation	*CISO and Crisis Communication*
Semester(s) in which the module is taught	*Winter*
Person responsible for the module	*Georges Ataya <ga@atayapartners.com> (Solvay Brussels), gataya@solvay.edu* *Evaldas Bruze <evaldas@l3ce.eu > (VMU, Kaunas)* *Diava Vitkute-Adzgaiskiene <daiva.vitkute@vdu.lt > (VMU, Kaunas)*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	Pre reading, lectures, case study, workshop and Coaching hours
Workload (incl. contact hours, self-study hours)	*Pre reading: (12 hours before and during the module delivery); Lectures (12*2 hours); Case study and workshop (6 hours over 12 weeks laps time in groups of students); module exam (2 hours in a multiple-Choice examination)* :
Credit points	5
Required and recommended prerequisites for joining the module	No additional requirements specific for this module.
Module summary	Cybersecurity Communication activities are essential in crisis situations and as regular communication of the CISO to stakeholders. Crisis communication is required for three specific focuses that are: Communicate to resolve the incident and the crisis; Communicate as a compliance notification required by law and regulators; and finally communicate to improve the reputation as a follow-up on an incident/crisis. Mastering communication activities is a must skill for cybersecurity leaders.
Module objectives/intended learning outcomes	**Learning outcomes that students should attain in the module in terms of:** **A. Knowledge: familiarisation with major communication requirements for the Cybersecurity in terms of:** **1. Regular leadership communication activities towards various stakeholders including senior management, users and regulators** **2. Crisis communication for the three purposes of containing the incident/crisis, of regulatory notification, and of preserving reputation.**

	3. Regular awareness activities as a n essential control for improving the preparedness of the Human Factor. **B. Skills: Possess the necessary skills to master the various actions related to planning, developing and conducting communication actions.** **C. Competences: Students must be able to create the communication plan including the design, the timeline, the identification of target audience, the definition of the communication channel, the identification of the message, the evaluation of the impact, and the improvement for a future cycle.**
Content	1. ***The purpose of the communication activities in terms of Audience and business results. The impact of communication on the protection, detection, response and recovery activities related to cybersecurity.*** 2. ***Communication elements including the objective, the expected impact, the target audience, the communication channel, and the timing. How to build a communication plan.*** 3. ***Building a dashboard as a baseline for communication to key stakeholders. Contents of a dashboard and alignment with the four Dimensions of the Balanced Scorecard model.*** 4. ***The crisis communication – Part 1: Principles of Incident/Crisis management*** 5. ***The crisis communication – Part 1: Communicate to resolve the incident/Crisis*** 6. ***The crisis communication – Part 2: Cybersecurity related regulations and their notification requirements (NIS2, DORA, GDPR, etc.)*** 7. ***The crisis communication – Part 2: Conduct regulatory communication requirements*** 8. ***The crisis communication – Part 3: Business needs for preserving reputation. Build reputation requirements in line with business objectives.*** 9. ***The crisis communication – Part 3: Validate cybersecurity and communication activities in line with not-accepted reputational risks. Develop actions along with management and business leaders.*** 10. ***Awareness program objectives, audience and plans*** 11. ***Cybersecurity awareness tools: Phishing and user reflexes exercises, alignment with key threats and vulnerabilities; awareness as a full protection mechanism.***

	12. Putting it all together: case studies on major communication actions and campaigns before and after an incident.
Exams and assessment formats	*Three written assignments after sessions 5, 7, and 9 related to the development of relevant communication plans. One final multiple-choice questionnaire.*
Study and examination requirements	*Requirements for successfully passing the module* *e.g. the final grade in the module is composed of 60% performance on exams, 10% quizzes, 10% take-home assignments, 10% in-class participation. Students must have a final grade of 60% or higher to pass*
Reading list	Best Practices for Cyber Crisis Management — ENISA (europa.eu) cybersecurity-incident-management-guide-EN.pdf (cybersecuritycoalition.be) Chapter 6. Communications to Promote Interest | Section 1. Developing a Plan for Communication | Main Section | Community Tool Box (ku.edu) 10 Crisis Communication Plan Examples (and How to Write Your Own) (hubspot.com) FIRSTCON23-TLPCLEAR-Benetis-ISO-27035-practical-value-for-CSIRTs-and-SOCs.pdf (PDF) Try to esCAPE from Cybersecurity Incidents! A Technology-Enhanced Educational Approach (researchgate.net) Try to esCAPE from Cybersecurity Incidents! A Technology-Enhanced Educational Approach July 2024 Rūta Pirta-Dreimane Agnė Brilingaitė Evita Roponena

Risk Management of Cyber-Physical Systems

Module designation	*Risk Management of Cyber-Physical Systems*
Semester(s) in which the module is taught	Spring (2/4)
Person responsible for the module	Paolo Trucco <paolo.trucco@polimi.it> (POLIMI)
Language	English
Relation to curriculum	Elective (CISO, RISK, EDU, THR)
Teaching methods	Lectures, Exercises, Assignments, Experiential learning (serious game)
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125* *Contact hours (please specify whether lecture, exercise, laboratory session, etc.): 50* *Private study, including examination preparation, specified in hours[1]: 75*
Credit points	*5*
Required and recommended prerequisites for joining the module	*None*
Module summary	*The **Risk Management of Cyber-Physical Systems** module aims to equip students with the skills to analyse, assess, and manage risks associated with socio-cyber-physical systems. It provides a comprehensive understanding of complexities and practices in technology risk governance (in the different stages of the system life cycle), and in operational resilience, through practical applications of industry-recognized methods, tools and processes. Students will analyse case studies and engage with a serious game to gain practical insights into the interplay between cybersecurity and business continuity. The module includes three core instructors and features guest lectures from industry professionals, offering valuable practitioner perspectives.*
Module objectives/intended learning outcomes	After successful completion of this course, students will be able to: • Identify and categorise technology risks of operating and digital technologies • Describe and prioritise risk and resilience features of socio-cyber-physical systems exposed to a variety of threats • Distinguish and compare approaches to and methods for technology risk governance at different system life

	cycle stages (from deign, to project management, to operations) • Select and apply the most appropriate risk assessment approach and methods given the features of the socio-cyber-physical system under analysis • Examine and evaluate the suitability of an organisation's technology risk governance model • Prepare a strategic report on technology risk assessment. • Describe the concepts and principles related to the Business Continuity Management (BCM), conduct Business Impact Analysis (BIA), identify and evaluate recovery strategies, develop Business Continuity Plans
Content	**12)** Course introduction. Risk management concept and process. Risk-based technology selection and adoption **[Trucco]** **12)** System safety engineering of cyber-physical systems. Risk Engineering methods: **[Trucco]** f) Failure Mode Effects and Criticality Analysis (FMECA) f) Fault Tree Analysis (FTA) f) Event Tree Analysis (ETA) f) Probabilistic Risk Analysis (PRA) **12)** Risk Analysis of Socio-Technical systems: Human and Organizational risk factors; Risk management of Organizational accidents; the High Reliability Organization theory. Critical incident analysis **[Trucco]** 12) Cyber Risk modelling **[Frumento]** f) Types of risks iii) Humans iii) IT iii) OT f) Cyber risk models and principles iii) Cyber risk models iii) Cascading effects iii) Correlation among risks iii) Risks of intangible assets **12)** Challenges and Advances in Industrial Cyber Risk Assessment **[4h – Frumento]** f) Information security Today f) Challenges in modern Security Governance f) Continuous risk assessment f) Principles of Social Engineering 12) Cyber risk maturity models and management **[4h – Frumento]** f) CMMs f) DevSecOps drill down iii) SCA iii) SBOM iii) Best practices f) EU Legislation framework f) US Legislation framework and comparison

	12) Case study by practitioners: Cybersecurity Threats, Strategy and Management at IntesaSanPaolo **[Trucco + Guest lecturer (Lonati)]** **12)** Case study by practitioners: Cyber and Physical Risk Management at SNAM spa **[Trucco + Guest lecturer (Chittaro)]** **12)** Business Continuity Management **[Petrenj]** f) BCM Fundamentals and business cases f) Business Impact Analysis f) Recovery strategies f) Collaborative BCM and SC resilience **12)** Business Continuity Management – serious game session 1 **[Petrenj]** **12)** Business Continuity Management – serious game session 2 **[Petrenj]** **12)** Cybersecurity for Critical Infrastructure **[Petrenj + Guest lecturer (Lazari)]** f) Importance of CIP-R f) Critical Infrastructure Resilience f) Interdependencies and cascading events f) Modelling and analysis of interdependent systems f) Cyber threats to CI f) Best practices and frameworks CIP-R
Exams and assessment formats	• A group written assignment: prepare either an essay on the state of art review of a relevant topic/challenge in the industrial cybersecurity risk management domain, or a Technology Risk Assessment report on an advanced digital technology. • Final written test, comprising few exercises and theoretical questions
Study and examination requirements	50% - Group written assignment 50% - Final written test
Reading list	• Bedford, Tim & Cooke, Roger M., "Probabilistic risk analysis: foundations and methods", Cambridge University Press, 2001. • Reason J., "Managing the risks of organisational accidents", Ashgate, 1997. • Hubbard, D. W., & Seiersen, R. (2023). How to measure anything in Cybersecurity Risk. *John Wiley & Sons, Inc*. • Course material: case texts, teaching notes and exercises, slides. • Suggested readings by the instructors.

Cybersecurity Auditing

Module designation	*Cybersecurity Auditing*
Semester(s) in which the module is taught	*Winter*

Person responsible for the module	*Georges Ataya <ga@atayapartners.com> (Solvay Brussels)*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	Pre reading, Lectures, Case study and workshop, Coaching hours
Workload (incl. contact hours, self-study hours)	*Pre reading: (12 hours before and during the module delivery); Lectures (12*2 hours); Case study and workshop (6 hours over 12 weeks laps time in groups of students); module exam (2 hours in a multiple-Choice examination)*
Credit points	5
Required and recommended prerequisites for joining the module	No additional requirements specific for this module.
Module summary	Auditing is a third line of defence that aims at giving assurance to decision makers in relation to the existence and the efficiency of controls. Auditing involves validating the activities already performed by the second line of defence (for example risk managers, Chief information security officers, IT operations team, Devops teams) and the first line of defence (Business operations and managers). Building an annual audit programme, developing an audit plan for specific audit assignments, and finally conducting the assignment and producing the resulting report. Auditing produce a statement of findings and recommendations aimed at improving the governance and operations of the cybersecurity activities.
Module objectives/intended learning outcomes	**Upon completion of this module, the learner will be able to develop an understanding of audit activities as an integral part of the assurance process. They will acquire practical skills to plan, develop and conduct comprehensive cyber security audit assignments. In addition, learners will be able to design audit plans tailored to the needs of stakeholders.** **Learning outcomes that students should attain in the module in terms of:** **LO1. Knowledge: familiarisation with audit activities as part of assurance process, including scoping, the selection of suitable criteria, the audit process and the audit reporting.** **LO2. Skills: Possess the necessary skills to master the various actions related to planning, developing and conducting a full audit assignment on Cybersecurity activities with the aim at informing stakeholders on the maturity, effectiveness and outcome of audit activities to**

	align with business requirements and good auditing and business practices. **LO3. Competences: Students must be able to create the audit plan, adjust the scoping of the assignment to business and technical needs or stakeholders request; Develop a scoping of the assignment; select a suitable criteria; align with usual audit practices including the Certificate in IT auditing.** **LO4. They must be able to develop audit fieldwork and produce a report with findings and recommendations.**
Content	1. ***The purpose of audit activities and the need for a third line of defence and relation with Internal auditing (e.g. external/internal auditing for certification), and relation with monitoring activities*** 2. ***The business and technical need of an audit assignment.*** 3. ***The scoping of the assignment and the selection of suitable criteria and a framework, a method or a baseline. Assess the possible use of automated tools.*** 4. ***The development of an audit plan including various phases and a description of various fieldwork activities.*** 5. ***The management of audit work includes the validation of the existence of controls, the validation of the effectiveness of controls, substantive testing and conducting interviews.*** 6. ***The development of an audit report aligning the findings, the recommendations and the opinion statement to respond to audit request and business needs. The method to produce SMART recommendations that aim at bringing optimal, most suitable and effective mitigations.*** 7. ***The presentation of audit findings to the audit requestor highlighting the impact and severity of the findings and the return on investment of proposed recommendations.*** 8. ***The development of a yearly audit program based on the understanding of an audit universe, an assessment of business needs from the assurance and audit activity and the best use of available audit resources.*** 9. ***Understand of the specificities of cybersecurity auditing with the aim at giving assurance of protection controls, the maturity of the organisation, and the efficiency of the second lines of defence (Risk management; project management Office; Compliance management; CISO office; DPO office) as well as governance practices (Senior management role and involvement in cybersecurity governance;***

	the cybersecurity spending effectiveness and justification). ***10. A business case with a real-life audit request to be developed in groups in various environment (Auditing the supply chain, the cybersecurity project implementation; the effectiveness of performance indicators and veracity of management reporting on cybersecurity posture; The effectiveness of intrusion detection activities; the effectiveness of awareness activities, etc.).*** ***11. Presentation of the business case in groups benefiting the whole class.*** ***12. A business case with a real-life need for developing a yearly audit program based on a given risk assessment and a typical audit universe)***
Exams and assessment formats	*Evaluation of both business cases in sessions 10 and 12. Multiple choice questions. An evaluation of a "bad" audit report.*
Study and examination requirements	*Requirements for successfully passing the module* *e.g. the final grade in the module is composed of 60% performance on exams, 10% quizzes, 10% take-home assignments, 10% in-class participation. Students must have a final grade of 60% or higher to pass*
Reading list	ITAF - IT Audit Framework from ISACA Store - An ITAF Approach to IT Audit Advisory Services | Digital | English - ISACA Portal- Six Benefits of a Cybersecurity Audit (and 6 Steps to Perform One) Author: Osman Azab, CISA, CISM, CRISC, CGEIT, CSAC Date Published: 16 January 2024 Six Benefits of a Cybersecurity Audit (and 6 Steps to Perform One) (isaca.org) IS Audit Basics: Auditing Cybersecurity Author: Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt, and R. V. Raghu, CISA, CRISC Date Published: 1 March 2019 IS Audit Basics: Auditing Cybersecurity (isaca.org) A Client-Centered Information Security and Cybersecurity Auditing Framework, Mario Antunes, Marisa Maximiano, Ricardo Gomes (PDF) A Client-Centered Information Security and Cybersecurity Auditing Framework (researchgate.net)

	Integrated framework for cybersecurity auditing October 2020 Information Security Journal A Global Perspective 30(2) DOI: 10.1080/19393555.2020.1834649 Iman M. A. Helal, Osamah Almatari, Sherif Mazen, Sherif Elhennawy Integrated framework for cybersecurity auditing | Request PDF (researchgate.net)

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Cybersecurity Economics & Supply Chain

Module designation	*Cybersecurity Economics & Supply Chain*
Semester(s) in which the module is taught	*second*
Person responsible for the module	*Marius Laurinaitis <laurinaitis@mruni.eu> (MRU)*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	The teaching methods include interactive lectures that provide theoretical foundations, supplemented by hands-on practical exercises to apply the concepts in real-world scenarios. Students are encouraged to engage in discussions and group work to foster collaboration and deepen their understanding. Additionally, case studies and scenario-based learning are utilized to analyze real cybersecurity incidents, enabling students to develop critical thinking and problem-solving skills. Presentations allow students to articulate their findings and demonstrate their understanding of key concepts, fostering a comprehensive learning experience that blends theory with practical application.
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload:* *Contact hours: 30 hours lesson* *Private study including examination preparation, specified in hours[1]: 95 hours*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Basic understanding of cybersecurity.*
Module summary	The *Cybersecurity Economics & Supply Chain* module aims to equip students with comprehensive knowledge of the economic aspects of information security and supply chain cybersecurity. It covers key concepts such as the direct and indirect costs of cyber incidents, the economic impact of various cyber threats on organizations, and the strategic role of cybersecurity in business planning. Students will explore frameworks, budget allocation for cybersecurity, and methods for managing third-party risks in supply chains. Through interactive lectures, practical exercises, and case studies, students will learn to conduct qualified investment analyses, understand technical incident reports, and apply economic models in security. Graduates will be able to strategically plan cybersecurity processes and evaluate the economic efficiency of security solutions within organizations and supply chains.

Module objectives/intended learning outcomes	*Upon successful completion of this module, students will be able to:* 1. **Understand Cybersecurity Economics.** Students will be able to analyze the economic implications of cybersecurity within organizations and incorporate cybersecurity considerations into business strategies. 2. **Assess the Costs of Cyber Incidents.** Students will develop skills to identify and evaluate the direct and indirect costs of cyber incidents, using case studies on data breaches, ransomware attacks, and other cybersecurity events. 3. **Analyze the Economic Impact of Cyber Threats.** Students will be equipped to evaluate how different types of cyber threats affect an organization's financial stability, reputation, and long-term growth prospects. 4. **Strategically Plan Cybersecurity Investments.** Students will learn to perform qualified investment analyses, make informed decisions about cybersecurity budgets, and determine the appropriate level of investment in prevention, detection, response, and recovery efforts. 5. **Apply Cybersecurity Frameworks and Standards.** Students will be able to utilize and critically assess various cybersecurity frameworks and standards. 6. **Manage Cybersecurity in Supply Chains.** Students will understand and manage the financial and strategic impact of cybersecurity risks across supply chains, particularly focusing on third-party risks and economic consequences. 7. **Anticipate Future Trends in Cybersecurity Economics.** Students will be prepared to explore and analyze emerging trends, technologies, and threats that shape the future of cybersecurity investments and the economic considerations within organizations. 8. **Effectively Communicate Findings.** Students will be capable of conducting comprehensive case analyses, preparing structured reports, and presenting their findings in a logical and sequential manner.
Content	This course provides knowledge on the economic aspects of information security, helping students understand and manage the financial implications associated with cyber threats and incidents. It aids in making informed investment decisions in security solutions and delving into descriptions of cyber threats and technical analyses of incidents. 1. Introduction to Cybersecurity Economics: Understanding the economic implications of cybersecurity within organizations. Overview of key concepts and the role of cybersecurity in business strategy. 2. Cost of Cyber Incidents: direct and indirect costs of cyber incidents. Case studies on data breaches, ransomware attacks, and other cybersecurity events.

	3. Economic Impact of Cyber Threats on Organizations: Exploring how different types of cyber threats (e.g., phishing, DDoS, malware) affect an organization's financial stability, reputation, and long-term growth. 4. Investment in Cybersecurity. How Much is Enough? Discussion on budget allocation for prevention, detection, response, and recovery. **5. Economics of Cybersecurity Frameworks and Standards.** 6. Supply Chain Cybersecurity Risks and Vulnerabilities. 7. Cybersecurity in the Supply Chain. Economic Implications. Understanding the financial and strategic impact of cybersecurity across supply chains. How to manage third-party risk and its economic consequences. 8. **Future Trends in Cybersecurity Economics**: Exploring emerging trends, technologies, and threats that will shape the future of cybersecurity investments and economic considerations in organizations.
Exams and assessment formats	*final exam (60 minutes)*
Study and examination requirements	Research Paper (25%): Evaluation of clear and logical presentation structure, adherence to presentation norms, comprehensive case analysis using multiple sources, and quality conclusions. •Report (25%): Evaluation of logical and sequential presentation of the incident situation, attention to the economic impact on the organization (if possible), appropriate segmentation of the incident's technical parts, and identification and allocation of compromise indicators. •Exam (50%):
Reading list	• ENISA Reports: Various resources on the economics of security and risk management. • Academic Papers: Including works by Anderson on the economic perspective of information security and Su's overview of economic approaches to information security management. • Practical Models: Such as the Return on Security Investment (ROSI) and other improvement models in IT security management. • Cybersecurity Frameworks: Including the Cyber Kill Chain and MITRE ATT&CK matrix. 1. Economics of Security: Facing the Challenges, ENISA, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/Experts_Contributions 2. 2. Economics of Security: Facing the Challenges, ENISA, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/EoS%20Final%20report/ 3. Security 3. Economics and the Internal Market, ENISA, https://www.enisa.europa.eu/publications/archive/economics-sec/ 4. 4. Anderson, R. (2001): Why Information Security is Hard - An Economic Perspective. In: ACSAC 2001: Proc. 17th Annual Computer Security

	Applications Conference, pages. 358–365. IEEE Press, Los Alamitos. Downloadable from: http://www.acsac.org/2001/papers/110.pdf 5. 5. Su, X. (2006). An overview of economic approaches to information security management. http://eprints.eemcs.utwente.nl/5693/01/00000177.pdf 6. Sonnenreich, W., Albanese, J., and Stout, B. (2006). Return on security investment (ROSI)-A practical quantitative model. Journal of Research and Practice in Information Technology, 38(1), pages 45-56. Downloadable from: http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf 7.Cavusoglu, H., 7. Cavusoglu, H. and Raghunathan, S. (2004): Economics of IT Security Management: Four Improvement 8. 8. Cyber kill chain, https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain 9. 9. MITRE ATT&CK matrix, https://attack.mitre.org/

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Cybersecurity Education and Training Delivery I

Module designation	*Cybersecurity Education and Training Delivery I*
Semester(s) in which the module is taught	*Optional course (1st or 2nd semester)*
Person responsible for the module	*Lisa Morávek <moraveklisa@vut.cz> (VUT)*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*lecture, lab, seminar*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload:* *Contact hours: lecture: 12 hours, seminar / discussions: 12 hours, practice / laboratory session: 24 hours - each session consists of 1 hour lecture (demo), 1 hour seminar / discussion and 2 hours of assisted lab / practice session* *Private study including examination preparation, specified in hours[1]: 64 hours - used for preparing for sessions, solving assignments, preparing for examination, self-study*
Credit points	*5*
Recommended prerequisites for joining the module	*Technological Foundations for CS & Security Controls*
Module summary	*3-4 sentences summarizing the objectives, content and methods. Something along the lines: "The Cybersecurity Education and Training Delivery module aims to prepare students to identify weaknesses, raise awareness and develop training programs in the realm of cybersecurity education. It presents an array of technical tools and modern methodology to teach cybersecurity related content while combining it with fundamental pedagogical principles. Students will be able to plan and carry out cybersecurity trainings, which will further be developed in the second module of this kind.*
Module objectives	*Knowledge* - *Understanding of different materials, delivery methods and infrastructure components used in cybersecurity education* - *Mapping trainee groups requirements with specific types of materials and delivery methods* *Skills* - *Developing materials for cybersecurity classes* - *Deploying the infrastructure for delivery of training materials* - *Using Git, GitHub to develop content* - *Using cyber range technologies for trainings* - *Creating interactive media content for cybersecurity topics*

	Competences - *Organizing a cybersecurity training content repository* - *Communicating relevance of topics part of a training / course* - *Assessing individual and group characteristics with respect to cybersecurity knowledge and skills* - *Providing personalized support to trainees*
intended learning outcomes	*Learning Outcomes:* *On successful completion of the component, the learners will be able to:* - *Critically evaluate appropriate methodologies and materials for cybersecurity education, training and awareness* - *Appraise students' needs to plan and carry out cybersecurity trainings using modern technologies and approaches, such as Cyber Ranges, Tabletops, etc.* - *Create new teaching material reflecting the relevance of emerging trends in cybersecurity and use modern technologies for their dissemination (Git, etc).*
Content	1. *Fundamentals of pedagogy and training* a. *principles of learning and motivation* b. *pedagogical standards and frameworks* 2. *Adult education and methodology* a. *Creating classes: accounts, permissions* b. *Publishing and advertising content* c. *Adult learning principles and behavioural change strategies* 3. *Modern Methods of Teaching and Trainings in cybersecurity: Materials, infrastructure and methods for teaching and training (in cybersecurity)* c) *Types of materials* c) *Typical infrastructure used for teaching and training* c) *Methods used in teaching cybersecurity topics* 4. *Collaborative tools in creating, maintaining and curating digital materials* a. *Types of digital collaboration tools* b. *Versioning and repositories of text / human readable content* c. *Office suites* 5. *Using Git and GitHub for version control* a. *Basic concepts of Git version control* b. *Common Git commands* c. *Using GitHub to store and publish Git-based content* 6. *Use of GitHub for collaboration* a. *Branches, pull requests, reviews*

	b. *Issues, wiki, discussions* c. *Organizations, projects, teams in GitHub* d. *Organizing a cybersecurity teaching / training class* i. *Using GitHub & Office suites or organize a class* i. *Structuring public and private content* i. *Controlling access to content and resources* 7. *Creating interactive and media digital content -* a. *Types of media content: pictures, audio, video* b. *Tools for creating and editing pictures (screenshots, diagrams, plots)* c. *Screen and audio recording* d. *Creating and editing video content* 8. *Using Cyber-Ranges in cybersecurity trainings I* a. *Demonstration of user-friendly, individualistic scenarios for training* b. *Introduction to platform featuring several simulations with virtual and physical polygons utilizing 5G infrastructure and other real-world technologies, such as IoT and Industry 4.0. (BUTCA)* 9. *Using Cyber-Ranges in cybersecurity trainings (BUTCA) II* a. *Creation of own scenarios for teaching purposes* 10. *Tabletop Exercises in Cybersecurity Trainings* 11. *Capstone project and out-of-class support* a. *Designing a cybersecurity training unit* b. *Using forums, mailing lists and text media for support* c. *Creating conference calls, recordings, vlogs* d. *Using Office suites and GitHub* e. *Engaging participants in content review* 12. *Assessment of participants cybersecurity classes + bug-bounty programs* a. *Using Cybersecurity challenges and practical items* b. *Types of examinations* c. *Evaluation and feedback, results analysis, success metrics* i. *Goals of feedback questions inside forms* i. *Processing feedback* i. *Processing student results* v. *Correlating results, planning for next iterations*
Exams and assessment formats	*Two take-home assignments (20% each)* - *Team Projects:* o *First assignment: Create a Git / GitHub repository with specified education contents*

	o *Second assignment: Prepare a scenario for cyber range* *Final exam (60 minutes)*
Study and examination requirements	*The final grade in the module is composed of 50% performance on exams, 40% take-home assignments, 10% in-class participation. Students must have a final grade of 50% or higher to pass*
Reading list	*Open Education Hub Methodology: https://open-education-hub.github.io/methodology/* *Cybersecurity Educational Resources: https://github.com/CSIRT-MU/edu-resources* "GitHub Docs" online manual. Link https://docs.github.com/en "GitHub Training Manual" Link: https://githubtraining.github.io/training-manual/#/

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Cybersecurity Education and Training Delivery II

Module designation	*Cybersecurity Education and Training Delivery II*
Semester(s) in which the module is taught	*(1st or 2nd semester)*
Person responsible for the module	*Răzvan Deaconescu (razvan.deaconescu@upb.ro) (UNSTPB)*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lecture, lab, seminar*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload:* *Contact hours: lecture: 12 hours, practice / laboratory session: 36 hours – each session consists of 1 hour lecture (mostly practical interactive demos) and 3 hours of assisted lab / practice session* *Private study including examination preparation, specified in hours[1]: 64 hours - used for preparing for sessions, solving assignments, preparing for examination, self-study*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Technological Foundations for CS & Security Controls* *Cybersecurity Education and Training Delivery I*
Module summary	*The "Cybsersecurity Education and Training Delivery II" module aims to build the required skills for students to be creators of practical cybsersecurity contests and use competition-based learning in their educator role. Students will learn how to design, implement, deploy and grade challenges as part of cybsersecurity contests (e.g. CTF – Capture the Flag). These are to be used as part of training and teaching activities that students will conduct themselves.*
Module objectives/intended learning outcomes	*On successful completion of this module the learner will be able to:* *LO1: Design practical cybersecurity exercises that serve as both a learning and a (self)assessment platform for participants* *LO2: Outline common patterns in cybersecurity attack and defense activities that can be replicated and integrated in cybersecurity exercises* *LO3: Develop, employ and asses practical cybersecurity exercises, both as single-topic challenges and as vulnerable boxes that feature a complex interconnected topics closer to a real-world setup* *LO4: Combine patterns from existing cybersecurity exercises into new customized deployments* *LO5: Assess student practical cybsersecurity knowledge and skills and revise exercises according to their current level*

	LO6: Design and set up cyber range-environments and CTF (Capture the Flag)-like contests, including setting up the platform, selecting challenges, grading, providing support *LO7: Summarize and interpret results and feedback of practice activities*
Content	1. *Overview of cybersecurity practice activities: wargames, CTF contests & challenges, vulnerable boxes* a. *Typical structure of a practice activity: root account, the flag* b. *Types of challenges and structure: box, jeopardy, attack-defense (red team-blue team)* c. *Sample challenges, sample sites, walkthroughs* 2. *Pedagogical Considerations Related to Practical Activities* a. *Practical exercises: definitions and roles* b. *Structuring practical exercises* c. *Four-step approach to teaching practical exercises* 3. *Cybersecurity Practice Arsenal* a. *Web challenges arsenal* b. *Binary files arsenal* c. *Crypto arsenal* d. *Forensics arsenal* 4. *CTF Cybersecurity Challenges* a. *Contents of a cybersecurity challenge* b. *Lifetime of a cybersecurity challenge* c. *Use cases for challenges as services* d. *Tips and tricks for reliable challenges as services* e. *Aftermath of a contest including a CTF cybersecurity challenges* 5. *Deployment of CTF Challenges* a. *Scripting the deployment of challenges* b. *Deploying challenges on a remote system* c. *Using containers for deployment* 6. *CTF Engines – CTFd.io* a. *CTF engines for contests* b. *Features of CTFd* c. *Sample deployment of CTF challenges* 7. *Pedagogical Aspects of Contests and Competitions* a. *Contests, Competitions, Gamification, role in learning* b. *Competition-based learning* c. *Designing a competition for learning* d. *Assessing results* 8. *Organizing and Deploying a CTF Contest* a. *Setting up a contest: dates, accounts, challenge selection, storyline, announcements* b. *Deploying challenges* c. *Providing support, hints, maintaining active communication* d. *Presenting results, awards* 9. *Using Virtual Machines*

	a. *Virtual machines, benefits of virtual machines* b. *Automating work with virtual machines* c. *Using virtual machines as vulnerable boxes* d. *Validating a challenge inside the virtual machine* 10. *Designing a Vulnerable Box Challenge* a. *Identifying vulnerabilities for challenge* b. *Designing the challenge* c. *Validating a challenge* d. *Packing a challenge for deployment* 11. *Deploying Vulnerable Boxes* a. *Using a vulnerable box to set up the challenge* b. *Packing a virtual machine* c. *Publishing a virtual machine* 12. *Assessment of Results of Cybersecurity Practice Activities* a. *Scoreboards for results* b. *Statistics of results: times, challenges solved, hints* c. *Adjustments to difficulty (points, rating)*
Exams and assessment formats	*Two take-home assignments (20% each)* - *Team projects* - *First assignment: Create and deploy 3 CTF challenges, review / solve other 3 CTF challenges (from other teams) - peer-review* - *Second assignment: Create and deploy a vulnerable virtual machine (vulnerable box); solve / review the deployment of another vulnerable box (from another team)* *Final exam: practical exam (3 hours): setting up the infrastructure for a CTF-like contests and a vulnerable virtual machine*
Study and examination requirements	*The final grade in the module is composed of 50% performance on exams, 40% take-home assignments, 10% in-class participation. Students must have a final grade of 50% or higher to pass*
Reading list	*Cybersecurity Educational Resources: https://github.com/CSIRT-MU/edu-resources* *CTFd.io: https://ctfd.io/* *VulnHub (Vulnerable Virtual Machines): https://vulnhub.com/* *TryHackMe: https://tryhackme.com/* *Running practical exrcises: https://facultyfocus.aoeducation.org/2018-03/assets/aof_booklet_running_a_practical_exercise.pdf* *Practical Pedagogy: 40 New Ways to Teach and Learn: https://www.routledge.com/Practical-Pedagogy-40-New-Ways-to-Teach-and-Learn/Sharples/p/book/9781138599819*

Cybersecurity in Industry – Security of OT and Cyber-Physical Systems

Module designation	*Cybersecurity in Industry – Security of OT and Cyber-Physical Systems*
Semester(s) in which the module is taught	5
Person responsible for the module	Enrico Frumento <enrico.frumento@cefriel.com> (Cefriel)
Language	English
Relation to curriculum	Elective
Teaching methods	Expert lectures, lessons, audiovisual resources, collaborative work, technical materials, seminars, case study discussions, and flipped classrooms. Virtual lessons 18h; Audiovisual teaching resources 4h; Mentorship 2h; Collaborative work 9h; Case studies 15h; Study of the basic material 36h; Flipped classroom (preparation) 50h; Reading the supplementary material 10h; Final Examination 3h; Flipped classroom (presentation) 3h
Workload (incl. contact hours, self-study hours)	(Estimated) Total workload: *150 hours* Contact Hours: *48 hours* Self-study: *96 hours* Examination: *6 hours*
Credit points	5 ECTS
Required and recommended prerequisites for joining the module	• Management & analytical skills, teamwork skills. • Fundamental theoretical knowledge of operating systems, computer networking, programming tools, and systems, • Basic understanding of the techniques for reverse code engineering, malware analysis and cyber risk modelling. • Basic understanding of the industrial control systems
Module summary	This module aims to equip learners with comprehensive knowledge and practical skills in OT (Operational Technology) security, highlighting the differences and overlaps with IT (Information Technology) security. The focus will be on understanding key principles, risk modelling, and the legal and regulatory landscape, alongside developing skills to analyse, evaluate, and implement effective security measures in industrial environments.
Module objectives/intended learning outcomes	**Learning Objectives**: This module provides a comprehensive overview of the essential knowledge, skills, and competencies necessary for addressing cybersecurity in Operational Technology (OT) environments, highlighting the unique challenges compared to IT security. It covers key concepts such as risk modeling specific to OT, legal and regulatory frameworks, and emerging technologies like AI, 5G, and IIoT. The ability to analyze OT's evolving threat landscape, assess industrial cyber risks, and evaluate real-world attack cases is emphasized, along with the need to apply relevant standards and best practices. Competencies include identifying vulnerabilities, synthesizing remediation measures, and managing continuous risk

<table>
<tr><td></td><td>assessments, all while navigating the complexities of modern OT security governance and human-related threats.

Learning Outcomes: On successful completion of this module, the learner will be able to:
LO1: Evaluate the principles and challenges of OT security, differentiate them from IT security, and align security strategies with industry standards and best practices.
LO2: Critically assess and compare the OT threat landscape with IT, including analysing specific tactics, techniques, and procedures used in OT-focused cyber-attacks.
LO3: Examine and evaluate recent case studies of cyber incidents in OT environments, drawing lessons on risk assessment and security countermeasures.
LO4: Analyse and apply relevant laws, regulations, and standards to develop robust OT security frameworks, incorporating the latest technological advancements such as AI, 5G, and IIoT.
LO5: Develop comprehensive risk models and security measures tailored to OT environments, ensuring effective governance and continuous risk assessment.
LO6: Assess the impact of human factors on OT security, identifying key vulnerabilities and synthesising remediation measures to strengthen the overall security posture.</td></tr>
<tr><td>Content</td><td><table>
<tr><th></th><th>Lecture</th><th>Content</th></tr>
<tr><td>1</td><td>The overlapping and differences between IT and OT security 1/2</td><td rowspan="2">The module introduces the basic concepts of OT security. Gartner defines Operational Technology (OT) as “hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events”. OT differs from IT in terms of functionalities, the culture of operators, and threats. OT is a novel and rapidly expanding area for cybercrime and industry. The number of attacks against OT infrastructures is increasing; the pandemic and the geopolitical crisis played a considerable role because of the acceleration of digital transformation. For example, the reduction of on-site staff put a strain on OT systems and the already limited resources and required</td></tr>
<tr><td>2</td><td>The overlapping and differences between IT and OT security 2/2</td></tr>
</table></td></tr>
</table>

			increased external connectivity. However, from a cybersecurity point of view, IT and OT need specific competence and sensibility. The primary need is an integrated approach that includes cybersecurity, physical and cyber-physical security, integrated cyber-risk estimation, and governance models spanning IT and OT domains.
	3	OT Threat Landscape	This module aims to increase comprehension of the OT threat landscape and its differences from the IT world. OT security is not an extension of IT security and requires a unique set of competencies. Nonetheless, threat actors use different Tactics and Procedures. Background knowledge, such as the ATT&CK framework, is presented.
	4	Tactics, techniques and procedures of the cybercrime and their evolutions 1/2	In the deep analysis of the tactics, techniques and procedures used by threat actors in the context of attacks against OT and cyber-physical systems. The specialised framework for industrial systems of the ATT&CK framework is used. The module also aims to perform reverse code engineering of the most prominent cases. According to the attendance, basic elements of reverse code engineering will be presented as a prerequisite to the malware analysis module. This module is intended for managerial profiles and not for technical profiles.
	5	Tactics, techniques and procedures of the cybercrime and their evolutions 2/2	
	6	Analysis of recent and paradigmatic attack cases and lessons learnt – flipped classroom 1/2	In this module, we'll look at different real-life examples, some of which come from students' homework. Students must study a piece of harmful software or a cyber-attack related to OT security. Then, students will share what they have learned with the rest of the class and the teachers in a flipped classroom approach.
	7	Analysis of recent and paradigmatic attack cases and lessons learnt – flipped classroom 2/2	

	8		This course is pivotal for understanding how to mitigate risks in integrated systems and protect against cyber and man-made threats. Even from a cyber risk modelling point of view, OT security is not an extension of IT security and requires a unique set of competencies. The module will analyse the differences among classic cyber risk modelling techniques and theory and modelling of cyber-physical systems, with particular attention to correlation among different types of risk and the cascading effects on non-cyber systems (e.g., risks of explosion, etc). The module also discussed the role of humans in human-related threats.
	9	Standards, best practices and EU laws for cybersecurity in the context of OT cybersecurity 1/2	Having a comprehensive view of the EU cybersecurity law framework specifically applicable to industry, the student will be able to determine if their industry and activities are subject to a particular piece of cybersecurity legislation, assess the extent of this applicability, and understand the key concepts and requirements necessary for achieving compliance and demonstrating accountability. EU laws that could specifically impact the industry in the Cybersecurity domain, such as the NIS 2 Directive, the Cybersecurity Act, the Cyber Resilience Act, the Medical Device Regulation(s), the EU Machinery Directive, and ISO reference standards such as ISO-62443.
	10	Standards, best practices and EU laws for cybersecurity in the context of OT cybersecurity 2/2	

	11	The impact of the new technologies 1/2	The field of OT is undergoing a phase of evolution where new solutions (e.g., AI, 5G, IIoT, Quantum Computing, Quantum Cryptography) are being developed. These new technologies particularly impact integrated IT and OT systems, where cyber risks could have cascading effects on non-cyber risks. The existing literature recognises the critical need for robust cybersecurity measures to safeguard against intentional threats and hybrid attacks. Traditional approaches often involve individually securing data flows, network layers, and software components, emphasising preventing unauthorised access and ensuring data integrity. The module will analyse and discuss the impact of these new technologies and present foreseen coming threats.
	12	The impact of the new technologies 2/2	
Exams and assessment formats	• Self-evaluation test: 2h (1h pre and 1h post-assessment) • Flipped classroom Works: 50h preparation + 3h presentation • Collaborative work: 9h • Final exam: 3h		
Study and examination requirements	• Continuous evaluation (Self-evaluation test, flipped classroom Works, Collaborative work) 50% • Final exam: 50% • Students must have a 60% or higher final grade to pass the exam.		
Reading list	• Douglas W. Hubbard, Richard Seiersen, "How to Measure Anything in Cybersecurity Risk", Wiley Press (2023) • Smita Jain, Vasantha Lakshmi, "IoT and OT Security Handbook: Assess risks, manage vulnerabilities, and monitor threats with Microsoft Defender for IoT", Packt Publishing (2023) • Otis Alexander, Misha Belisle, Jacob Steele, "MITRE ATT&CK for Industrial Control Systems: Design and Philosophy", MITRE (2020) • Course material: case texts, teaching notes and exercises, slides. • Suggested readings by the instructors.		

Cybersecurity Law & Data Sovereignty (BUT)

Module designation	*Cybersecurity Law & Data Sovereignty (BUT)*
Semester(s) in which the module is taught	*summer*
Person responsible for the module	*Pavel Loutocký (BUT);*
Language	*English*
Relation to curriculum	*Specialisation, Ellective*
Teaching methods	*lesson*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload:* *Contact hours: 24 hours lesson* *Work hours - private study including examination preparation, specified in hours[1]: 95 hours*
Credit points	*5*
Required and recommended prerequisites for joining the module	*Basic understanding of cybersecurity principles, computer networks, and foundational knowledge of legal frameworks.*
Module objectives/intended learning outcomes	This course provides students with a comprehensive understanding of cybersecurity measures and related cybercrime aspects with a focus on EU regulation and international tools. Additionally, it covers data sovereignty, teaching students the regulations surrounding data handling, digital identity, and maintaining integrity in electronic document management. On successful completion of this module the learner will be able to: LO1: Understand and apply cybersecurity measures: Students will be able to understand and implement preventive and regulative measures in cybersecurity, particularly within the frameworks especially of the NIS 2 Directive, Cyber Resilience Act, Cyber Solidarity Act, and Cybersecurity Act. Students will also be able to work with and asses the regulatory framework based on particular case studies.

	LO2: Assess cybersecurity legal frameworks: Students will critically assess the links between national legal regulatory frameworks and international harmonization instruments in cybersecurity. LO3: Deploy legal tools for cybersecurity incidents: Students will be able to use legal tools and processes for handling and reporting cybersecurity incidents, especially in collaboration with cybersecurity incident response teams. LO4: Understand cybercrime investigation and prosecution: Students will comprehend the legal tools and processes for investigating and prosecuting cybercrime, particularly through international instruments like the Budapest Convention. LO5: Handle and transfer electronic evidence: Students will gain the ability to navigate European rules and procedures regarding the production and transfer of electronic evidence and understand its relevance in legal cases including relevant case law. LO6: Understand data sovereignty regulations: Students will be familiar with various legal regimes for data handling, including personal data transfer, electronic document management, and digital identity, with a focus on retaining integrity through the chain of custody.
Content	***Cybersecurity and Cybercrime*** *The content of this part of the module will cover the main concepts and structure of the cybersecurity law and criminal law applicable to cybercrime. The first area will include the theory and practice of cybersecurity obligations based on category of the regulated subject; liability for cybersecurity incidents; relevant case law; and tools for coordination and standardisation of cybersecurity compliance, such as cybersecurity certification. In the second area, we will cover relevant legal provisions of substantive and procedural criminal law; categorisation of cybercrimes; as well as European and international procedural tools used in investigation and prosecution of cybercrime.* ***Data Sovereignty*** *This part of the module is aimed at an in-depth exploration of the legal dimensions of specific aspects of data sovereignty and specific regimes applicable under the EU law. It prepares students to navigate the complex legal landscape in specific areas connected to various forms of data flows, in order to be able to ensure compliance in their professional practices within the EU. Apart from the regulatory regimes for processing personal data, participating in data spaces or doing business through online platforms, the content will include rules and requirements applicable to handling of electronic documents, including the relevance for constituting electronic evidence, and to the use of electronic identification and digital identity in particular in its application in the public law processes.*
Exams and assessment formats	*final open book exam (2 hours)*
Study and examination requirements	*Requirements for successfully passing the module:* *the final grade in the module is composed of 60% performance on exam(s), 10% class assignments, 20% in-class participation. Students must have a final grade of 60% or higher to pass in the exam.*

Reading list	DAIMI, K., ALSADOON, A., PEOPLES, C., EL MADHOUN, N. Emerging Trends in Cybersecurity Applications. Springer. 2023. Available online for free: https://link.springer.com/book/10.1007/978-3-031-09640-2 LEHTO, M., NEITTAANMÄKI, P. Cyber Security. Critical Infrastructure Protection. Springer. 2022. Available online for free: https://link.springer.com/book/10.1007/978-3-030-91293-2#bibliographic-information NIST. National Checklist Program (NCP), 2022. (https://ncp.nist.gov/repository) FIRST CSIRT Services Framework. 2019. (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1)

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Machine and Deep Learning in Cybersecurity

Module designation	*Machine and Deep Learning in Cybersecurity*
Semester(s) in which the module is taught	*3rd or 4th*
Person responsible for the module	*Prof. Sanda Martinčić-Ipšić, PhD <smarti@uniri.hr> (UNIRI)* *Prof. Marina Ivašić-Kos, PhD <marinai@uniri.hr> (UNIRI)*
Language	*English*
Relation to curriculum	*elective* *Cyber Threat Intelligence Specialist*
Teaching methods	*The teaching and learning strategy will consist of lectures, exercises, and focused activities such as videos, tutorials, case studies, practical assignments, and project work.* *Each week, students will attend a one-hour live lecture and a one-hour tutorial session with a hands-on demonstration of the practical part of the lecture. During the class, participants will be given tasks and exercises related to the covered content to be able to connect theory with practice. The live sessions will mainly involve explaining theoretical concepts with an emphasis on practical application to best use the lecturer's expertise in the classroom. Students will additionally have 2 hours of online activities every week aimed at mastering the concepts covered in the weekly topics. Directed activities consist of reading selected chapters from the book, listening to parts of the content in the form of videos, solving practical tasks, and solving homework that will be given in the exercises.* *Students will benefit from mentoring and formative feedback on completed activities and projects during class. All module resources will be available to students in a structured format through the LMS.*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload:* ***150 hours*** *Contact hours (please specify whether lecture, exercise, laboratory session, etc.):* ***Synchronous Lectures: 12 hours*** ***Tutorial Sessions: 12 hours*** ***Directed e-Learning Activities: 24 hours*** ***Independent learning and work on project: 102 hours***
Credit points	*5*
Required and recommended prerequisites for joining the module	*Finished course: Automation of security tasks and data analytics*
Module summary	This module focuses on applying machine learning and deep learning techniques to cybersecurity challenges such as anomaly

	and malware detection, fraud detection, and spam classification. Students will explore various machine learning algorithms, analyze their performance, and design appropriate models for specific cybersecurity tasks. The course also covers explainability issues in AI-driven cybersecurity, alongside hands-on labs using Python and popular libraries like Scikit-learn, TensorFlow, and PyTorch.
Module objectives/intended learning outcomes	*It is expected that after successfully completion of this module and fulfilling all the prescribed obligations, the student will be able to:* *LO1. Compare the advantages and disadvantages of basic machine learning algorithms, especially those related to classification, clustering, and time series analysis.* *LO2. Analyse and apply appropriate machine learning methods when solving specific problems such as anomaly or malware detection* *LO3. Analyse and select deep learning methods that are suitable for the given task in the field of cybersecurity, such as spam detection, and credit card fraud detection.* *LO4. Evaluate the performance of the model and, based on that, choose the best machine or deep learning model for a given problem in the field of cybersecurity* *LO5. Design and apply a machine or deep learning model for a self-defined problem in the field of cybersecurity* *LO6. Discuss the possibility of applying machine or deep learning in cybersecurity and explain related problems such as explainability, interpretability, transparency, personal data protection, and legal and ethical challenges.*
Content	**12-Week Program: Classes:** _____ **Week 1: Introduction to Data Analytics and Machine Learning in Cybersecurity** • **Lecture:** Overview of ML in cybersecurity, Benefits, and challenges, use of cloud cases, mobile applications, and IoT. Anomaly detection, Malware detection, Ethical and legal aspects of AI • **Tutorial/ Lab:** Introduction to Python for machine learning: Scikit-learn, PyOD (Python Outlier Detection), Matplotlib, XGBoost, Prophet, **Week 2**: **Unsupervised machine learning: Clustering** • **Lecture:** K-means, distance measures, Hierarchical clustering, elbow method, dimensionality reduction, PCA, t-SNE

	• **Tutorial/ Lab:** Apply K-means clustering, and identify outliers based on the distance from the cluster centroids. Visualize the clusters and anomalies using scatter plots. Compare different distance measures. Apply hierarchical clustering (agglomerative). Visualize the dendrogram to identify clusters. Calculate the within-cluster sum of squares (WCSS) for each K, plot the WCSS values against the number of clusters to create the elbow plot. Apply PCA to reduce the dimensionality of features. Apply t-sne. **Week 3: Supervised machine learning: Classification** • **Lecture:** Decision trees, features, Partitioning train-test set. Cross-validation. Evaluation: accuracy, precision, recall, F-score, AUROC, Confusion matrix. Naïve Bayes, k-nearest neighbours • **Tutorial/ Lab:** Build a decision tree classifier using Scikit-learn. Visualize the decision tree to interpret the rules and splits. Partition dataset for the training-testing. Perform k-fold cross-validation. Evaluate the model. Calculate accuracy, precision, recall, and F-score, AUROC. Visualize the confusion matrix using a heatmap. Apply Naïve Bayes, k-nearest neighbours evaluate and compare results. **Week 4: Supervised machine learning: Classification** • **Lecture:** Support Vector Machines (SVM). Ensembles, Bagging. Boosting, Random Forest (RF). Feature importance. XGBoost • **Tutorial/ Lab:** Build SVM and random forest classifier using Scikit-learn. Feature importance Train XGBoost model. Tune the hyperparameters (e.g., learning rate, number of boosting rounds). Visualize classes. Unbalanced classes. **Week 5: Time series analysis** • **Lecture:** Trends, Seasons, Cycles. Smoothing, moving average (MA), Autoregressive Integrated Moving Average (ARIMA), Seasonal ARIMA (SARIMA). Evaluation: Mean Absolute Error (MAE): Mean Squared Error (MSE): Root Mean Squared Error (RMSE), R-squared (R^2), • **Tutorial/ Lab:** Fit time series model with Prophet. Fine-tune Prophet model parameters and evaluate performance MAE. MSE, RMSE, R2. Visualize. Apply seasonality and holidays. **Week 6: Anomaly detection** • **Lecture:** Unbalanced classes, fraud detection, intrusion detection, false positives vs. false negatives, feature engineering, time series detection, goodness of fit, and density-based methods. Isolation forest. • **Tutorial/ Lab:** Anomaly detection applications in Cybersecurity: Network Intrusion Detection, Fraud Detection, and System

	Monitoring. Apply Z-score normalization. Apply Isolation Forest and One-Class SVM for anomaly detection. Use prophet for time series analysis of anomalies. **Week 7: Neural networks** • **Lecture:** Artificial Neural Networks (neurons, layers, hidden layers, activation functions). Perceptron. A Multi-layer Perceptron. Feed-forward network. Detecting spam emails using MLP. Backpropagation. Evaluation metrics. • **Tutorial/ Lab:** Perceptron. Multi-layer perceptron. Testing the influence of different network structure and different activation functions to network performances on spam detection. **Week 8**: **Introduction to Deep Neural Networks** • **Lecture:** Basic architecture of Deep Neural Network. Network hyperparameters. Training of neural network. Epochs. Loss function. Analysing Results. Credit Card Fraud detection using deep neural network. • **Tutorial/ Lab:** Using environments and services to define deep neural network architecture (e.g. TensorFlow, Keras, PyTorch, Google Colab). Training of neural network for credit card fraud detection. Analysing Results. **Week 9: Biometric authentication** • **Lecture:** Convolutional neural networks (CNN). Biometric authentication using CNN. Data augmentation. Transfer learning. Optimization algorithms. Parameter regularization. Overfitting and generalization. • **Tutorial/ Lab:** Creating a simple deep convolutional neural network for biometric authentication, training the model and testing the influence of various hyper parameters and learning parameters to network performances. Evaluate performance using standard metrics. **Week 10: Adversarial Machine Learning** • **Lecture:** Adversarial attacks (Poisoning attacks, Evasion attacks, Model extraction attacks). Adversarial Machine Learning Examples. Popular Adversarial Attack Methods. Generative Adversarial networks (GAN). Deep fake. • **Tutorial/ Lab:** Using Deep fake and different GAN models for adversarial attacks on image classification. **Week 11: Transformers and emerging topics**

	• **Lecture:** Typical deep learning architectures and appropriate tasks (Recurrent neural network (RNN). Long Short-Term Memory (LSTM). Autoencoders. Attention. Transformers. Large language models. Using transformers for different cybersecurity tasks. • **Tutorial/ Lab:** Using different transformer networks and testing them on user behaviour analytic and biometric authentication tasks. **Week 12: Overview of Course Material, Class Discussion & Guest Lecture (optional)**
Exams and assessment formats	***Two midterm assessments*** • 1. online quiz ML in week 7 (LO1, LO2, LO4, LO6) • 2. online quiz DL in week 12 (LO3, LO4, LO5, LO6) ***Weekly (1,2,3,4,5,6,8,9,10,11) short computer-based quizzes*** (LO1 - LO6) ***Project* assignment** on selected ML topic in cybersecurity (e.g. anomaly detection, credit card fraud detection, (image) malware detection, biometric authentication, adversarial attack,…) with technical report and oral presentation (LO1 - LO6)
Study and examination requirements	*Requirements for successfully passing the module* *the final grade in the module is composed of 40% performance on two midterms (50% needed to pass), 10% weekly quizzes, 50% project assignment (30% practical work, 10% oral presentation, 10% technical documentation).* *Students must have a final grade of 60% or higher to pass*
Reading list	***Recommended books.*** *Clarence Chio, David Freeman: Machine Learning and Security: Protecting Systems with Data and Algorithms, O'Riley, 2018.* *Marwan Omar, Machine Learning for Cybersecurity, Springer, 2022.* *Ian Goodfellow, Yoshua Bengio, Aaron Courville Deep Learning (Adaptive Computation and Machine Learning series), The MIT Press, 2016.* *Emmanuel Tsukerman, Machine Learning for Cybersecurity Cookbook. Over 80 recipes on how to implement machine learning algorithms for building security systems using Python;Packt 2019.* ***Supplementary Books*** *Soma Halder and Sinan Ozdemir. Hands-On Machine Learning for Cybersecurity, Packt, 2018.* *Rajvardhan Oak, 10 Machine Learning Blueprints You Should Know for Cybersecurity, Packt 2023.*

	Francois Chollet, Deep Learning with Python, Second Edition 2nd Edition, Manning, 2021. ***LAB resources:*** *scikit-learn - Machine Learning in Python https://scikit-learn.org/stable/* *PyOD documentation! https://pyod.readthedocs.io/en/latest/* *XGBoost Documentation https://xgboost.readthedocs.io/en/stable/* *Prophet forecasting https://facebook.github.io/prophet/* TensorFlow https://www.tensorflow.org/ Keras https://keras.io/ PyTorch https://pytorch.org/ Google Colab https://colab.google/

Digital Forensics, Chain of Custody and eDiscovery

Module designation	*Digital Forensics, Chain of Custody and eDiscovery*
Semester(s) in which the module is taught	*Full Time*: *Semester 2 (Year 1) or Semester 1 (Year 2) or Semester 2 (Year 2)* *Part Time (Option I)*: *Semester 3 (Year 1) or Semester 2 (Year 2) or Semester 3 (Year 2) or Semester 1 (Year 3)* *Part Time (Option II)*: *Semester 2 (Year 1) or Semester 3 (Year 1) or Semester 1 (Year 2) or Semester 2 (Year 2)*
Person responsible for the module	*Michael Bradford < michael.bradford@ncirl.ie> (NCI)*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*The teaching and learning strategy will consist of classes and directed activities such as videos, tutorials, case studies and discussions on the programme's Learning Management System (LMS). Each week students will begin by engaging with 1 hour of directed online activities aimed at introducing threshold concepts for that week's topic. Directed activities consist of short digestible pieces of content, such as explanatory videos, reading, guided tutorials, etc. Learners will then attend a live 1-hour lecture and a 1-hour tutorial session. Learners will be assigned tasks and exercises related to the directed content so that they can connect the theory to practice. Live sessions will mostly be practically based so as to make best use of the lecturer's expertise in the classroom. Learners will benefit from mentoring and formative feedback on completed directed activities during classes. All module resources are made available to learners in a structured format via the LMS.*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload: 125 hours* *Directed e-Learning Activities: 12 hours* *Synchronous Lectures: 12 hours* *Tutorial Sessions: 12 hours* *Private study including examination preparation, specified in hours : 89 hours*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Law, Compliance, Governance, Policy, and Ethics*
Module summary	*This module aims to enable learners to develop a knowledge, skills and competence to approach a Digital Forensics investigation whilst safe-*

<table>
<tr><td></td><td>guarding the chain of custody of acquired digital forensic evidence. This module also aims to develop skills associated with eDiscovery. Learners will gain practical experience in using various tools used in Windows forensics, Linux forensics, mobile forensics, network forensics and eDiscovery. This module provides an in-depth coverage of various sub-domains of digital forensics and how it is related to eDiscovery.</td></tr>
<tr><td>Module objectives/intended learning outcomes</td><td>The Digital Forensics, Chain of Custody and eDiscovery module is intended to enable learners to develop knowledge, skills, and competences in digital forensics, as well as eDiscovery. From a practical perspective, learners develop expertise on a range of tools associated with mobile, network and the digital forensics of various operating systems. Furthermore, learners investigate and assess digital forensic case studies.

On successful completion of this module the learner will be able to:
LO1: Demonstrate in-depth critical awareness and interpretation of laws, compliance requirements, methods and procedures used in digital forensics investigations.
LO2: Carry out a forensic investigation of operating systems, mobile devices and networks, critically analyse the evidence and document the findings in a report.
LO3: Compare, evaluate and use forensic tools to forensically analyse digital devices.
LO4: Carry out an eDiscovery engagement across multiple platforms making use of various electronic discovery tools.
LO5: Critically analyse the results of an eDiscovery review, prepare production sets, write reports, and appraise the concepts for information retrieval and enterprise search technologies.</td></tr>
<tr><td>Content</td><td>
<table>
<tr><th></th><th>Lecture Topic</th><th>Detail</th></tr>
<tr><td>1</td><td>Introduction</td><td>Introduction to the module.
Principles of forensics, need of digital forensics, background to digital forensics, Computer crime.
Categories of incidents.
Cybercrime investigation.
Scenarios of eDiscovery and digital forensics investigations.</td></tr>
<tr><td>2</td><td>Digital forensics models and methodologies.</td><td>Digital evidence.
Direct and circumstantial evidence.
Types of data (content and non-content).
The digital forensics process.
Exemplar models and methodologies.</td></tr>
</table>
</td></tr>
</table>

			Standards and best practices.
	3	Digital Evidence	Sources of digital evidence and the investigation process. Evidence handling rules. ACPO principles of computer related evidence. Legal and ethical obligations. Handling digital evidence (Identification, Collection, Acquisition, Preservation) Triage and anti-forensics. Chain of custody. Need to maintain extensive documentation. Digital evidence admissibility (Assessment, Consideration, and Determination) Digital forensics report writing, typical parts, letter of findings, affidavits.
	4	Forensic Tools	Types of computer forensic tools, various tasks performed by forensic tools and its details. Drive imaging. Password cracking tools. Forensic workstation, choosing the forensic toolkit. Validating and testing forensic software, using NIST tools. Cloud platform challenges and considerations.
	5	Windows Forensics	Importance of operating system forensics. Relevant windows data structures. History of the windows registry, registry editor key, registry information. Tracking user activity by analysing shellbags and quick access/Recent Files Review bitlocker encryption and location of recovery keys.

	6	Network Forensics	Basics of network forensics When to apply network forensics. Key elements in communication. Network trace. Key concepts to interpret a network trace. IP and MAC addresses and networking infrastructure. Show how session keys (perfect forward secrecy) encryption/decryption works with RSA .Public Key encryption. Explain the role of deep packet inspection and web application firewalls in a network.
	7	Mobile Device Forensics	Mobile devices, mobile phones in crime, collecting a phone for analysis, data recovered from a mobile phone. Components of mobile phone. Accessing the data from a mobile phone. Tools used for mobile forensic analysis.
	8	Linux Forensics	Linux shell, linux boot sequence. Filesystems and disk/directory Encryption techniques. Important directories and sub-directories. File deletion in linux. Find Recently accesses/modified/changed files Log analysis /var/log/*
	9	Introduction to Electronic Discovery & Enterprise Search	What is discovery, how is conventional discovery different to eDiscovery. What is electronic discovery. Common challenges of electronic discovery. Examine Microsoft Purview or Gcloud Vault , eDiscovery platforms. Discuss Full-text search, Faceting, Nearest-Neighbour/Clustering. Highlighting of hits.

			Rich document handling. Document fields and schema design.
	10	Electronic Discovery Reference Model	Discussing various phases of Electronic discovery reference model in detail. Information governance. Deduplication, keyword searching, technology assisted review (TAR), email threading, textual near duplicate identification.
	11	Electronic Discovery Processes	Approaches to eDiscovery. Forms of electronically stored information. What constitutes evidence and what is metadata. Selecting an eDiscovery tool. Significance of quality assurance in eDiscovery practices. Email archiving/journaling.
	12	Revision, catch-up and formative feedback	

Exams and assessment formats

The summative assessment strategy for this module is shown in the table below.

Assessment Type	***Assessment Description***	***Outcome addressed***	***%***	***Assessment Date***
Continuous Assessment 1	*This assessment will consist of practical tasks in the form of a homework. This will assess learners' knowledge and competences on digital forensic processes, concepts and various tools used in digital investigations.*	*LO1, LO2, LO3*	*50*	*Week 6*
Continuous Assessment 2	*An assessment that will assess learner's knowledge and analytical skills regarding enterprise search and eDiscovery rules, processes, and platforms. Learners will*	*LO4, LO5*	*50*	*Week 11*

	<table><tr><td></td><td>conduct practical activities using various tools and write a report on their work.</td><td></td><td></td><td></td></tr></table> *Reassessment strategy:* *The reassessment strategy for this module will consist of an assessment that will evaluate all learning outcomes.*
Study and examination requirements	*Learners must have an overall final grade of 40% or higher to pass this module.*
Reading list	*Recommended Book Reading* • *G. Johansen, 2020, Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats, 2nd edition, Packt Publishing [ISBN: 978-1838649005]* • *J. Seitz, T. Arnold (2021) Black Hat Python, 2nd Edition: Python Programming for Hackers and Pentesters, No Starch Press, [ISBN: 978-1718501126]* *Supplementary Book Reading* • *H. Carvey. (2016), Windows Registry Forensics, 2nd Edition, Syngress. [ISBN: 978-0128032916]* • *N. Jaswal (2019), Hands-On Network Forensics: Investigate network attacks and find evidence using common network forensic tools. Packt Publishing, [ISBN: 978-1789344523]* *Other Resources* • *[website], CD-ROM: Live CD for Forensics, http://www.caine-live.net/* • *[website], Forensic articles, http://www.forensickb.com/* • *[website], COMPUTER FORENSIC RESOURCES, http://www.evestigate.com/COMPUTER%20FOR ENSIC%20RESOURCES.htm* • *[website], Security Journals/Whitepapers https://securityjournaluk.com/* • *[website], Forensic Focus, http://www.forensicfocus.com* • *[website], Sans, http://www.sans.org* • *[website] AI Powered Search. https://livebook.manning.com/book/ai-powered-search/about-this-meap/v-9/* • *[website], Guide: Good Practice Discovery Guide - CLAI, https://clai.ie/wp-content/uploads/2021/10/CLAI-Good-Practice-Discovery-Guide-v2_0.pdf* • *[website], Relativity One Discovery User Guide. https://help.relativity.com/RelativityOne/Content/index.htm* • *[website], Microsoft Purview, Microsoft365 eDiscovery. https://learn.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide*

	• *[website] Apache Lucene Solr https://github.com/mikeroyal/Apache-Lucene-Solr-Guide* • *[website], Autopsy Sleuth Kit. https://www.sleuthkit.org/autopsy/* • *[website], Nist forensic sample images. https://cfreds.nist.gov/* • *[website] Linux forensics cheatsheet http://www.security-hive.com/post/linux-forensics-the-complete-cheatsheet*

Ethical Hacking & Penetration Testing

Module designation	*Ethical Hacking & Penetration Testing*
Semester(s) in which the module is taught	*4*
Person responsible for the module	*Fidel Paniagua <fidel.paniagua@unir.net> (UNIR)*
Language	*English*
Relation to curriculum	*elective*
Teaching methods	*Lab works, virtual lessons, audiovisual resources, collaborative work, mentorship, technical material, self-evaluation.*
Workload (incl. contact hours, self-study hours)	*Total workload: 5 ECTS (150 hours)* *Contact hours:* – *Virtual lessons: 15 h.* – *Audiovisual teaching resources: 6 h.* – *Mentorship: 16 h.* – *Collaborative work: 7 h.* – *Case studies: 17 h.* *Self-study:* – *Study of the basic material: 60 h.* – *Reading the supplementary material: 45 h.* – *Lab works: 10 h.* – *Self-evaluation test: 4 h.*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Management & analytical skills, basic knowledge of auditing processes (e.g., DEMING cycle), teamwork skills, planning and leadership skills. Fundamental theorical knowledge of operating systems, computer networking, and programming tools and systems.*
Module summary	*This module will allow the student to understand, analyze and manage the ethical hacking process by learning the concepts, techniques and processes through videos, practical exercises and laboratories. Obtaining the ability to use the results of an audit for management and decision making.*
Module objectives/intended learning outcomes	*On successful completion of this module the learner will be able to:* 1. *Knows the basic principles, the importance of ethical hacking and system auditing, the methodologies and*

	techniques, also the laws, policies and legal aspects carried during the Ethical Hacking process. 2. *Analyse and manage the methodologies and techniques used in ethical hacking.* 3. *Recognize how it works the tools used to perform ethical hacking audit, and its results.* 4. *Explain the importance of ethical hacking practices and describe the methodologies used for penetration testing in various environments.* 5. *Develop skills for analysis to identification and mitigation process for vulnerabilities in computer systems.* 6. *Identify threats and attack methodologies during the develop of and ethical Hacking audit.* 7. *Analyse the security posture of systems by identifying vulnerabilities and distinguishing between different types of cyber-attacks.* 8. *Manage the technical and executive reports for taking decisions level.* *Skills:* *Manage ethical hacking audit processes by selecting specific attacks according to the results we need to obtain.* *-Planning and manage the ethical hacking process.* *-Elaborate results reports after Ethical Hacking process, for the taking decision level.*
Content	*<u>1. Ethical hacking fundamentals (history & main concepts)</u>* • *Description: Description of the History and fundamentals of the Ethical Hacking process, and its evolution, regulations and policies.* • *Level of difficulty: medium* *<u>2. Operating systems vulnerabilities & attack vectors</u>* • *Description: Description of the OS vulnerabilities and attack vectors, methodology of identification, detection, and neutralization. (Methods, tools, and procedures)* • *Level of difficulty: medium* *<u>3. Network vulnerabilities & attack vectors (IT, IoT, OT)</u>* • *Description: Description of the network vulnerabilities and attack vectors, methodology of identification, detection, and neutralization. (Methods, tools, and procedures)* • *Level of difficulty: medium* *<u>4. Web vulnerabilities & attack vectors</u>*

	• *Description: Description of the Web vulnerabilities and attack vectors, methodology of identification, detection, and neutralization. (Methods, tools, and procedures)* • *Level of difficulty: medium* *5. Cloud vulnerabilities & attack vectors* • *Description: Description of the Cloud vulnerabilities and attack vectors, methodology of identification, detection, and neutralization. (Methods, tools, and procedures)* • *Level of difficulty: medium* *6. Pentesting methodologies* • *Description: Theorical description of the types of different methodologies to develop a pentesting, the stages and requirements for it, and the generation and interpretation of executive and technical reports.* • *Level of difficulty: low* *7. Footprinting and reconnaissance* • *Description: Fundamental description of the process for reconnaissance and footprinting stage, the tools used and the concepts to apply in an ethical hacking audit.* • *Level of difficulty: medium* *8. Vulnerability analysis and exploitation tools* • *Description: Description and explanation of the vulnerability analysis, the tools used for analysis, and the tools for exploitation. Interpretation of the analysis.* • *Level of difficulty: low* *9. Ethics and legislation in ethical hacking* • *Description: Definition and explanation of the laws, regulations, and policies for an ethical hacking process. (national and International)* • *Level of difficulty: low* *10. Ethical Hacking certification roadmap:* • *Description: Introduction to the certification in Ethical Haking (study preparation, in technical and theorical aspects)* • *Level of difficulty: low*
Exams and assessment formats	*Self-evaluation test: 4 h.* *Lab Works: 10 h.*

	Collaborative work: 7 h. *Final exam: 2 h.*
Study and examination requirements	*Continuous evaluation (Self-evaluation test,* *Lab Works, Collaborative work) 40%* *Final exam: 60%*
Reading list	*EC-Council. (2016). Certified Ethical Hacker (CEH) V9: Ethical Hacking and Countermeasures. EC-Council.* *Palmer, C. (2015). Ethical Hacking and Penetration Testing Guide. McGraw-Hill Education.* *Engebretson, P. (2014). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Syngress.* *Simpson, K., & Peck, M. (2019). Ethical Hacking for Beginners: Learn the Basics of Security, Hacking, and Penetration Testing. Independently published.* *Oriyano, S. (2019). Ethical Hacking: A Comprehensive Beginner's Guide to Learn and Master Ethical Hacking. Independently published.* *Anand, N. (2020). Ethical Hacking: Ethical Hacking and Penetration Testing Guide. Independently published.* *Han, D., & Singh, A. K. (2021). Ethical Hacking: Learn the Fundamentals of Web Security, Network Security, and Ethical Hacking. Independently published.* *Brown, J. M. (2018). Ethical Hacking: A Hands-On Introduction to Breaking In. Addison-Wesley Professional.* *Dieterle, D. A. (2018). Ethical Hacking and Penetration Testing: A Hands-On Introduction to Hacking. Packt Publishing.* *Smith, S. (2017). Ethical Hacking: The Ultimate Beginner's Guide to Using Penetration Testing to Audit and Improve the Cyber Security of Computer Networks, Including Tips on Social Engineering. CreateSpace Independent Publishing Platform.*

Malware Analysis

Module designation	*Malware Analysis*
Semester(s) in which the module is taught	*4*
Person responsible for the module	*Fidel Paniagua <fidel.paniagua@unir.net> (UNIR)*
Language	*English*
Relation to curriculum	*elective*
Teaching methods	*Lab works, virtual lessons, audiovisual resources, collaborative work, mentorship, technical material, self-evaluation.*
Workload (incl. contact hours, self-study hours)	*Total workload: 5 ECTS (150 hours)* *Contact hours:* – *Virtual lessons: 15 h* – *Audiovisual teaching resources: 6 h.* – *Mentorship: 16 h.* – *Collaborative work: 7 h.* – *Case studies: 17 h.* *Self-study:* – *Study of the basic material: 60 h.* – *Reading the supplementary material: 45 h.* – *Lab works: 8 h.* – *Self-evaluation test: 4 h.*
Credit points	*5 ECTS*
Required and recommended prerequisites for joining the module	*Management & analytical skills, basic knowledge of auditing processes (e.g., DEMING cycle), teamwork skills, planning and leadership skills. Fundamental theorical knowledge of operating systems, computer networking, and programming tools and systems.*
Module summary	*This module will allow the student to understand, analyze and manage the malware analysis process by learning the methods, techniques and tools used. With exercises, videos and laboratories the student will learn the importance and how to use the results for auditing and other cybersecurity processes.*
Module objectives/intended learning outcomes	*On successful completion of this module the learner will be able to:* 1. *Knows the history of malware and its evolution, regulations and policies. Defining key concepts related to malware, such as types of malwares, malware lifecycles, and common infection methods.*

	2. *Comprehend the Malware analysis process.* 3. *Classify the different types of malwares according to different criteria.* 4. *Recognize how it works the tools used to malware analysis process, and its results.* 5. *Identify the methods used for the malware analysis process, what are the tools and programs to develop a malware analysis.* 6. *Plan and execute the process for malware analysis.* 7. *Analyse the structure and functionality of malware by dissecting code, identifying malicious behaviours, and determining potential damage or security risks.* 8. *Elaborate reports with the results of the malware analysis, for organizational levels* *Skills* *-Evaluate and analyse types of anti-malware solutions according to their performance and know the main malware campaigns to apply preventive measures.* *- Manage the malware analysis process during critical time, helping the business resilience plan.* *-Develop results reports after malware analysis, for the management taking decision level.*
Content	*1. <u>Malware analysis introduction and fundamentals:</u>* • *Description: Introduction to the context of malware analysis. Understanding the structure, operation, and interaction of malware, the importance of the process for malware analysis, to provides valuable information not only for the design and development of effective countermeasures, but also for understanding the origin of an attack and the ability to assess whether an organization's security systems can detect it and therefore analyse and take the necessary and appropriate response actions.* *Level of difficulty: low* *2. <u>Malware analysis methodologies:</u>* • *Description: This topic focuses on the study of a "Malware Analysis and Reverse Engineering" methodology using malware analysis and reengineering techniques and methods whose main objective is to acquire knowledge and gain a complete understanding of a particular malware, its operation, identification and ways to remove it.* *Level of difficulty: medium*

	3. Malware analysis tools: • *Description: fundamental explanation and description of the different tools used for developing the malware analysis process.* *Level of difficulty: medium* *4. Anti-Malware tools:* • *Description: Fundamental explanation and description of the actual anti-malware tools.* *Level of difficulty: medium* *5. Case studies: Malware scenarios* • *Description: Simulate malware to learn how it works under controlled conditions.* *Level of difficulty: low* *6. Malware crisis management:* • *Description: Methodological description of the process and procedures for the malware analysis process (preparation, action, execution, dissemination and feedback) communication for resilience business plan.* *Level of difficulty: medium* *7. Malware analyst certification roadmap:* • *Description: Introduction to the certification in malware analysis. (study preparation, in technical and theorical aspects)* *Level of difficulty: low*
Exams and assessment formats	*Self-evaluation test: 4 h.* *Lab Works: 10 h.* *Collaborative work: 7 h.* *Final exam: 2 h.*
Study and examination requirements	*Continuous evaluation (Self-evaluation test,* *Lab Works, Collaborative work) 40%* *Final exam: 60%*
Reading list	*Bermejo, J., Abad, C., Bermejo, J. R., Sicilia, M. A., y Sicilia, J. A. (2020). Systematic Approach to Malware Analysis (SAMA). Appl. Sci., 10(4), 1360. https://doi.org/10.3390/app10041360*

	Monnappa, K. A. (2018). Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware. Packt Publishing Ltd. *de Vicente Mohino, J. J., Bermejo-Higuera, J., Bermejo Higuera, J. R., Sicilia, J. A., Sánchez Rubio, M., & Martínez Herraiz, J. J. (2021). MMALE a methodology for malware analysis in linux environments. Computers, Materials & Continua, 67(2), 1447-1469.* *Masid, A. G., Higuera, J. B., Higuera, J. R. B., & Montalvo, J. A. S. (2023). Application of the SAMA methodology to Ryuk malware. Journal of Computer Virology and Hacking Techniques, 19(2), 165-198.* *Gregg, M. (2008). Build Your Own Security Lab: A Field Guide for Network Testing. Wiley Publishing.* *Hale Ligh, M., Adair, S., Hartstein, B., and Richard, M. (2011). Malware Analyst's Cookbook and DVD. Tools and Techniques for Fighting Malicious Code. Wiley Publishing, Inc.* *Sikorki, M., and Honing, A. (2012). Practical Malware Analysis. The hans-on guide dissecting malicious software. No Starch Press.* *Casey, E. (2013). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.* *Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2018). Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley.* *Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press.* *Mandiant. (2014). M-Trends: The Advanced Persistent Threat. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-m-trends-2014.pdf* *Dhar, P., & Mohanta, B. K. (Eds.). (2019). Malware Forensics: Investigating and Analyzing Malicious Code. CRC Press.*

	Russinovich, M. E., & Solomon, D. A. (2012). Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (6th ed.). Microsoft Press. *Rouse, M. (2018). Malware (malicious software). Retrieved from https://searchsecurity.techtarget.com/definition/malware-malicious-software* *Rogers, M., & Gregg, N. (2012). Practical Mobile Forensics (1st ed.). Packt Publishing.* *IEEE Computer Society. (2015). Malware Analyst's Guide to Network Analysis. IEEE Computer Society Press.* *Harris, S. (2019). The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory (2nd ed.). Wiley.*

Threat Intelligence

Module designation	*Threat Intelligence*
Semester(s) in which the module is taught	*3rd or 4th semester*
Person responsible for the module	*Radu Mantu <radu.mantu@upb.ro> (UNSTPB)*
Language	*English*
Relation to curriculum	*Elective*
Teaching methods	*Lesson, lab works, assignments*
Workload (incl. contact hours, self-study hours)	*(Estimated) Total workload:* ***150h*** *Contact hours (please specify whether lecture, exercise, laboratory session, etc.):* ***lesson=10h, lab=20h, assignments=20h*** *Private study including examination preparation, specified in hours[1]:* ***100h***
Credit points	*5*
Required and recommended prerequisites for joining the module	*Familiarity with Linux distributions, Python scripting* *Knowledge of C/C++, OS design is desirable*
Module summary	This module aims to introduce the fundamentals of Cyber Threat Intelligence (CTI). The lectures will present the CTI lifecycle, highlight strategic integration and discuss emerging trends in this field. The students will learn how to identify threat intelligence data streams, apply the extracted information for vulnerability assessment and threat mitigation, and disseminate newly acquired knowledge into public databases.
Module objectives/intended learning outcomes	**Learning Outcomes**: On successful completion of this module, the learner will be able to: - **LO1:** Recognize different types of cyber threats and apply analytical techniques to assess their potential impact. - **LO2:** Gather threat data from open-source and proprietary sources, as well as structure it according to their needs. - **LO3:** Incorporate threat intelligence into (automated) incident response processes, improving the detection, investigation, and mitigation of attacks.

	- **LO4:** Use specialized platforms and tools to analyze threat data and share relevant information. - **LO5:** Utilize the acquired intelligence to guide proactive threat hunting efforts with the goal of identifying potential compromises and indicators of attack.
Content	***Week 1:*** *Introduction to Cyber Threat Intelligence (CTI)* - ***Lecture:*** *Overview of CTI and its role in a modern security strategy. Present open-source / commercial threat intelligence feeds.* - ***Lab:*** *Deploy aggregators for threat intelligence data streams. Probe for emerging threats based on geolocation and other factors.* - ***Difficulty:*** *Introductory* ***Week 2:*** *CTI lifecycle and cybersecurity frameworks* - ***Lecture:*** *Present the phases of CTI and best practices to be applied at each stage. Discuss how CTI fits into frameworks such as MITRE ATT&CK and its integration with other areas in cybersecurity.* - ***Lab:*** *Become familiar with popular formats / schemas used in specifying Indicators of Compromise (IOC).* - ***Difficulty****: Introductory* ***Week 3:*** *Strategic planning* - ***Lecture:*** *Describe how to align CTI with the security goals and policies of an organization. Explain how to present security-related findings to non-technical stakeholders.* - ***Lab:*** *Automate information extraction from public databases and use OSS to generate reports.* - ***Difficulty****: Introductory* ***Week 4:*** *Vulnerability management* - ***Lecture:*** *Correlate threat intelligence with vulnerability detection to prioritize patching and mitigation. Present CVE databases.* - ***Lab:*** *Perform static, targeted malware detection based on publicly available signatures. Extend verification to an entire system.* - ***Difficulty:*** *Introductory* ***Week 5:*** *Advanced threat actor profiling* - ***Lecture:*** *Explain the notion of Threat Actors and how to build Adversary Profiles using historical data and behavioural patterns.* - ***Lab:*** *Generate rotating network captures for arbitrary time frames. Investigate user activity and automatically extract identifying features. Discuss honeypots.* - ***Difficulty:*** *Intermediate* ***Week 6:*** *Incident Response*

	- ***Lecture:*** *Present how CTI is used to guide Incident Response efforts. Discuss Intrusion Detection and Prevention Systems (IDP / IPS).* - ***Lab:*** *Configure an IDS / IPS to generate events or actively block traffic. Discuss its integration with the Linux network stack & the Netfilter Framework while considering the performance impact.* - ***Difficulty:*** *Advanced* ***Week 7:*** *The role of auditing in CTI* - ***Lecture:*** *Discuss the importance of data collection during the CTI lifecycle, as well as its analysis and dissemination. Present new approaches in this field, such as Data Provenance.* - ***Lab:*** *Introduction to the Linux audit system and its configuration for detecting anomalous behaviour.* - ***Difficulty:*** *Intermediate* ***Week 8:*** *Automation using Elastic Stack* - ***Lecture****: Introduction to Elastic Stack.* - ***Focus:*** *Configure the Logstash pipeline to collect and parse log entries from different sources. Pass the processed log data to an Elasticsearch cluster and visualise it via Kibana.* - ***Difficulty:*** *Advanced* ***Week 9:*** *Emerging trends and the future of CTI* - ***Lecture:*** *Present challenges facing CTI today. Discuss methods of applying Machine Learning techniques for the purpose of achieving predictive threat intelligence.* - ***Lab:*** *Introduction to containers and microservice environments. Present technical challenges created by namespaces and how to overcome them. Discuss methods of applying these solutions to Virtual Machine images.* - ***Difficulty:*** *Advanced* ***Week 10:*** *Review* - ***Lecture:*** *(optional) Guest speaker. Exam prep.* - ***Lab:*** *Review of previous activities.* - ***Difficulty:*** *N\A*
Exams and assessment formats	***Two home assignments (~10h each) and a final exam (~4h)***
Study and examination requirements	*Final grade composed of:* - ***40% performance on exam*** - ***30% lab activity*** - ***20% assignments*** - ***10% class participation*** *Students must have a final grade of* ***50% or higher*** *to pass.*

Reading list	***Mandatory Reading:*** - *"The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence"* - *"The Diamond Model of Intrusion Analysis"* - *"Intelligence-Driven Incident Response: Outwitting the Adversary"*

[1] When calculating contact time, each contact hour is counted as a full hour because the organisation of the schedule, moving from room to room, and individual questions to lecturers after the class, all mean that about 60 minutes should be counted.

Exam Study Regulations

Digital4Security
Shaping Europe's cyber future

Project details: Joint Master's Degree Programme
in Cybersecurity Management & Data Sovereignty (Digital4Security)

Project ID: 101123430

Call: DIGITAL-2022-SKILLS-03

Table of Contents

About the Digital4Security project

Digital4Security is a ground-breaking pan-European master's program aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. This €20m industry-led Master's, supported by funding from the DIGITAL Europe Programme, is a four-year initiative that comprises a Consortium of 36 partners spanning 12 countries. This master program will provide comprehensive knowledge of cybersecurity management, regulatory compliance, and technical expertise to European SMEs and companies.

Digital4Security is launching a collective cybersecurity revolution by harnessing the collective skill sets of our international Consortium, and the next generation of practical experts in the digital space. We're reskilling and upskilling graduates, professionals, managers and business leaders to become 'cyber confident', equipped to protect and empower European SMEs in the face of global cyber threats.

The Digital4Security curriculum is grounded in a rigorous needs analysis process involving all of our Consortium partners. The programme will blend academic and industry content to ensure graduates are equipped with both theoretical and job-ready cyber skills to fast-track employment. The program is designed to meet European accreditation standards and a wide range of national standards, with plans to offer micro-credentials for each module and industry certification in collaboration with our industry partners.

The Digital4Security Consortium

The Digital4Security Consortium is a dynamic pan-European partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management programme, developed and delivered by the best cybersecurity talent from Europe and worldwide. Table 1 lists the Higher Education Institutions (HEIs) jointly offering the master's degree, while Table 2 presents additional consortium partners, including industry stakeholders.

Table 1: Academic Partners (Higher Education Institutes) Offering the Joint Degree Program

No.	Partner	Abbreviation	Country
1	Universitatea Nationala de Stiinta si Technologies Politehnica Bucuresti	POLITEHNICA B.	Romania
2	National College of Ireland	NCI	Ireland
3	German University of Digital Science gGmbH	UDS	Germany
4	University of Rijeka	UNIRI	Croatia
5	Università degli Studi di Brescia	UNIBS	Italy
6	Politecnico di Milano	POLIMI	Italy
7	Universität Koblenz	UNI KO	Germany
8	CY Cergy Paris Université	CY	France
9	Mykolo Romerio Universitetas	MRU	Lithuania
10	Universidad Internacional de La Rioja	UNIR	Spain
11	Brno University of Technology	BUT	Czech Republic
12	Munster Technological University	MTU	Ireland
13	Vytautas Magnus University	VMU	Lithuania

Table 2: Associate Partners

No.	Associated Partner	Abbreviation	Country
14	DIGITAL TECHNOLOGY SKILLS LIMITED	DTSL	Ireland
15	IT@CORK ASSOCIATION LIMITED LBG	IT@CORK	Ireland
16	SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	SKILLNET	Ireland
17	ADECCO FORMAZIONE SRL	ADECCO TRAINING	Italy
18	ADECCO ITALIA HOLDING DI PARTECIPAZIONE E SERVIZI SPA	ADECCO GROUP	Italy
19	ADECCO ITALIA SPA	Adecco Italia	Italy
20	CEFRIEL SOCIETA CONSORTILE A RESPONSABILITA LIMITATA SOCIETA BENEFIT	CEFRIEL	Italy
21	ATAYA & PARTNERS	Ataya	Belgium
22	CYBER RANGES LTD	Cyber Ranges	Cyprus
23	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	FHG	Germany
24	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	NASK	Poland
25	POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	CMIP	Poland
26	SCHUMAN ASSOCIATES SCRL	SA	Belgium
27	CONTRADER SRL	Contrader	Italy
28	INDEPENDENT PICTURES LIMITED	indiepics	Ireland
29	MATRIX INTERNET APPLICATIONS LIMITED	MATRIX	Ireland
30	PROFIL KLETT D.O.O.	PROFIL KLETT	Croatia
31	SERVICENOW IRELAND LIMITED	ServiceNow	Ireland
32	EUROPEAN DIGITAL SME ALLIANCE	DIGITAL SME	Belgium
33	DIGITALEUROPE AISBL*	DIGITALEUROPE	Belgium
34	TERAWE TECHNOLOGIES LIMITED	TERAWE	Ireland
35	BANCO SANTANDER SA	BANCO SANTANDER /Santander	Spain
36	RED OPEN S.R.L.	RED OPEN S.R.L.	Italy

The HEIs, in conjunction with the Digital4Security consortium's industry partners, have collaborated and cooperated to jointly develop and design this programme and its curriculum.

Admission

The Admission Process commences upon each passing of application deadline dates, as is going to be published on the DIGITAL4Security website (https://www.digital4security.eu). Applications for admission must be submitted prior to the published deadline by means of the online application made through the DIGITAL4Security website. Notwithstanding the requirement for candidates to have made their applications prior to stated deadlines, at the discretion of the Joint Admissions Board (and only if there are still places available).

Admission will be on the condition that the candidate has satisfied the requirements of these regulations in terms of knowledge, skills, and competence by the end of the admission date, supported by all necessary documentary requirements. The Joint Admissions Board shall assess the knowledge, skills, and competence of candidates to determine whether the prospective student can be admitted to the programme. Working collaboratively with the Joint Admissions Board, the Secretariat will perform an initial review of applications to ensure the application is complete and meets the minimum set of requirements to make the candidate eligible.

Admission is open to bachelor graduates from non-technical backgrounds (e.g., economics, law, business) or those in mid/senior-level technical/business roles. Students who have not yet obtained their Bachelor degree at the time of the selection procedure but who would normally do so before the Master's degree programme begins, may be granted provisional admission. Students must submit a declaration from the relevant authorities that they have satisfied the requirements of a Bachelor degree before the start of the degree programme.

Joint Admission Board

The Joint Admissions Board, operating under the supervision of the Master's Board of Directors, is responsible for the selection and admission of the students to the degree programme. The Joint Admissions Board consists of (at least) one representative from each HEI partner. A chairperson and a secretary are nominated from among the representatives.

Requirements

Candidates are accepted onto the programme based on the quality of their education and professional background, their previous experience, and their linguistic capabilities and English language skills.

Admission may be granted to applicants who meet the following common admission criteria:

- Applicants are required to hold a minimum of a EQF Level 6 qualification.
- Applicants who have graduated from programs lacking embedded technical problem-solving skills must show additional technical proficiency and problem-solving abilities beyond their EQF Level 6 qualifications. This can be demonstrated through industry certifications, further qualifications, or certified professional experience. Those who do not meet these criteria will be subject to an interview and further assessment to determine their suitability for the programme.

- Since the program is delivered entirely online, applicants are required to have the necessary computing equipment, such as a laptop or desktop PC, that meets the minimum specifications, as stated on the programmes website. Additionally, applicants must ensure they have reliable internet access.
- Practical experience working in a business environment is valued.
- Practical experience in a scientific or technology domain is valued.
- All required application details, relevant information, and necessary documentation have been submitted by the applicant.
- The selection criteria for applications includes several factors: the applicant's motivation, academic achievements, and qualifications (including type and level), proficiency in language, research experience (including type and level), and professional experience.
- Applicants meet Recognition of Prior Learning (RPL) policy requirements (see section Recognition of Prior Learning Policy).

Language Qualification Requirements

The programme is delivered through English, as such, applicants whose first language is not English must attach a certified qualification of proficiency in English or exhibit proficiency in English through either a test and/or an interview. Table 3 shows the qualifications that fulfils the programme's minimum requirements for admission.

Table 3. Minimum Language Proficiency Requirements

IELTS	TOEFL (IBT)	CEF
6.5	90	B2

Compensation of Missing Prior Knowledge - Recognition of Prior Learning

Regulations for the compensation of missing prior knowledge are implemented for the programme. They provide for the consideration of applicants with lower, or no formal qualifications, currently working in a relevant field, for admission onto the programme.

Recognition of Prior Learning (RPL) is a policy that credits learning acquired before formally enrolling in a course or programme, derived from formal education, work, volunteering, or life experiences. RPL assesses and recognizes the relevance of a student's existing skills and knowledge to their current studies, potentially granting academic credits. This allows students to bypass certain course components, saving time and money. RPL is especially beneficial for admitting students who may not meet traditional academic requirements. The process includes evaluating the skills, knowledge, and experience through reviews of work portfolios, interviews, and practical assessments. Applicants submit portfolios detailing their relevant experiences, professional training, and certifications. RPL assessors then match these against course requirements. If equivalent, this prior learning can replace formal qualifications for admission. Should there be any gaps, the institution may recommend bridging courses to prepare the student

for full admission. Once validated, these competencies allow the student to enrol, ensuring that individuals don't repeat learning where they already demonstrate competence.

Applicants who do not have the minimum academic qualifications will be assessed for entry based on prior learning and work experience, combined with a demonstrated commitment towards meeting the academic requirements of the programme. Entry will be assessed using a written application from the candidate and by interview. Recognition of Prior Learning will be assessed in accordance with this policy, this may require a portfolio of evidence (this may include but is not limited to submission of an essay, references, examination results, and module/micro-credential/programme/training syllabi completed by the applicant) and interview, or other assessment as determined by the Joint Admissions Board.

The Joint Admissions Board's determination that an applicant has the necessary numeracy skills will be based on the evidence provided. Typically, the determination of a sufficient numeracy skill level will be based on prior completion of modules/micro-credentials/programmes/training with a high degree of numerical/mathematical subject content (e.g., Statistics, Probability, Calculus, Operations Research, Quantitative Techniques, Econometrics, Optimisation, Discrete Mathematics, Accountancy, Financial Analysis etc.).

Where there is insufficient evidence of numeracy skills, applicants may be required to complete an assessment to determine their suitability to the programme. Applicants require the ability to use mathematical understanding and skills to solve problems. Applicants need to be able to think and communicate quantitatively, to make sense of data, to have a spatial awareness, to understand patterns and sequences, and to recognise situations where mathematical reasoning can be applied to solve problems. Correspondingly, the assessment would focus on an applicant's capabilities in these areas.

Non-standard applicants may have extensive work/life experiences, which allied to their own natural learning ability and commitment would merit access to the programme and credit within it for the learning gained through their work/life experiences.

The term "learning" implies a conceptual as well as practical grasp of the knowledge or competence required. It should be applicable outside the environment in which it was acquired. Experience is not what is being evaluated but learning.

Applications for RPL consideration are made directly through the centralised admissions platform. All applicants seeking RPL entry are interviewed and requested to produce a portfolio describing the prior experience in the context of potentially creditable learning outcomes. The portfolio is considered by the programme director and the Admissions committee / Programme Directors Committee. The portfolio is evaluated and compared against the module to provide evidence of:

- *Validity*: Does the evidence supplied meet all/part of the outcomes/assessment criteria?
- *Sufficiency*: Is the evidence sufficient proof of the outcomes or assessment criteria?
- *Currency*: Is the evidence recent? The expectation is that learners experience or qualifications have been gained within the last 3 years.
- *Authenticity*: Is the evidence provided the learners own work?

In assessing whether learning gained from experience matches learning outcomes for a particular module, the assessors apply the following criteria:

- Has the appropriate balance between theory and practical application been attained?

- Is the learning achieved transferable?
- Has the appropriate academic level of learning been achieved?

Necessary Documentation for Application

All applications must be made online via the DIGITAL4Security website in accordance with the instructions and before the deadlines as stated on the website. Applications (at a minimum) must include the following documents:

- A copy of the applicant's passport (only the main pages),
- A certified copy of Diploma(s) (with official translation(s) into English if original(s) not in English) and, if available, a copy of the Diploma Supplement(s),
- Certified copies of academic transcripts (with official translation(s) into English if original(s) not in English),
- A Curriculum Vitae in English (preferably adhering to the Europass model)
- Official proof of English language abilities (where applicable),

Additional documents typically required include:

- Two letters of recommendation,
- A personal statement outlining the applicant's motivation and career goals,
- Proof or confirmation of availability of necessary hardware, software, and internet infrastructure for participation in the online study

Examinations Board

The Examinations Board is headed by the Master's Board of Directors. The Master's Board is responsible for the overall quality and standards of the degree programme and for agreeing upon the academic standards. It monitors the partner HEIs' compliance and is responsible for the degree programme being delivered to the highest academic standards. The Examinations Board may be supplemented with additional nominees from partner institutions who have expertise in quality assurance and those who are responsible for programme examination administration. Meetings of the Examinations Board shall convene after each programme examination session and after a provision of adequate time for grading and assessment of learners' exam scripts, project submissions, or other relevant coursework by programme faculty.

The Examinations Board deliberates cases, brought to its attention with at least one week notice. If the nature of the case brought to its attention demands a swift ruling, a special meeting may be arranged or written consultation of its members via electronically mediated systems instead. All assessments are conducted in accordance with the jointly agreed policies and procedures for the degree programme as adopted by the Master's Board.

Period of Study

The Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty is composed of 120 ECTS and may be delivered according to either Full Time or Part Time over 3 years with 30 ECTS or 20 ECTS respectively per Semester. Table 4 provides information of the expected period of study for each of these delivery schedules.

Table 4. Expected Duration of the Degree Programme

Name	Mode of Study	Intake rhythm	Average time required to complete studies
Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty	Full time	Each semester	4 semesters / 2 years
	Part time	Each semester	6 semesters / 3 years

Study load for the programme is expressed in credits of the European Credit Transfer and Accumulation System (ECTS) with 1 ECTS equivalent to an average of 25 hours of study.

Curriculum and Modules

Learning Goals

Graduates of the programme are expected to have achieved the Overarching Learning Goals in Table 3. They were developed to align with industry feedback and the analysis of related programmes internationally:

Table 3: Overarching Learning Goals across the Joint Degree Program

No.	Goal
PO1	Critically assess and evaluate cybersecurity principles, practices, and technologies relevant to modern enterprises.
PO2	Strategically apply cybersecurity knowledge and utilise practical skills and technologies for long-term success in cybersecurity leadership roles across diverse industries, government agencies, and institutional settings.
PO3	Identify knowledge gaps and undertake self-learning to acquire new knowledge to support professional development and the ability to adapt to evolving threats, technologies, and regulatory environments.
PO4	Exhibit and apply leadership skills necessary for effectively managing cybersecurity initiatives within organisations, including education and training, strategic planning, and resource allocation.
PO5	Critically evaluate and analyse cyber threats in order to implement effective security operations, and to enable the proactive identification, assessment, and mitigation of cyber threats.
PO6	Effectively apply analytical and strategic thinking in order to make decisions to address security requirements.
PO7	Communicate effectively across a range of complex and advanced cybersecurity concepts to provide leadership within an organisation and facilitate effective collaboration and teamwork.

PO8	Critically assess cybersecurity legal, information governance, and regulatory frameworks and practices to ensure effective oversight, auditing, risk mitigation, accountability, compliance, and strategic alignment with organisational objectives.

Modules

This Master's programme is delivered online and it composed of 120 ECTS organized in 2 modules: 95 ECTS obtained by mandatory modules and a set of 14 elective modules to complete for training. Table 5 provides information for each of the programme's modules on i) the ECTS allocation, ii) the mandatory/elective status, and iii) the corresponding partner institute.

Note: the elective modules that are offered for learners to choose from in any given semester may be restricted due to operational scheduling constraints and/or the overall learner demand for choosing particular elective modules. Notwithstanding this, the programme team will endeavour to accommodate the broadest offering of elective modules each semester under these constraints.

Table 5. Module ECTS, Mandatory/Elective Status, and Corresponding Partner Institute

No.	SUBJECT	ECTS	MAND/ELECT	PARTNER
1	AI & Emerging Topics in Cybersecurity	10	Mandatory	UDS
2	Business Resilience, Incident Management, and Threat Response	10	Mandatory	NCI
3	Cybersecurity Culture, Strategy & Leadership	5	Mandatory	VMU
4	Dissertation / Internship	25	Mandatory	UNI KO
5	Enterprise Architecture, Infrastructure Design and Cloud Computing	10	Mandatory	MTU
6	Law, Compliance, Governance, Policy, and Ethics	10	Mandatory	UNIBS
7	Research Methods	5	Mandatory	UNI KO
8	Security Operations	10	Mandatory	CY CERGY

9	Technological Foundations for CS & Security Controls	10	Mandatory	UPB
10	Automation of Security Tasks and data analytics	5	Elective	UNIRI
11	CISO and Crisis Communication	5	Elective	VMU
12	Risk Management of Cyberphysical Systems	5	Elective	POLIMI/ CEFRIEL
13	Cybersecurity Auditing	5	Elective	VMU
14	Cybersecurity Economics & Supply Chain	5	Elective	MRU
15	Cybersecurity Education & Training Delivery I	5	Elective	BUT
16	Cybersecurity Education & Training Delivery II	5	Elective	UPB
17	Cybersecurity in Industry - Security of OT and Cyber-Physical Systems	5	Elective	POLIMI
18	Cybersecurity Law & Data Sovereignty	5	Elective	BUT
19	Machine and Deep Learning in Cybersecurity	5	Elective	UNIRI
20	Digital Forensics, Chain of Custody and eDiscovery	5	Elective	NCI
21	Ethical Hacking & Penetration Testing	5	Elective	UNIR
22	Malware Analysis	5	Elective	UNIR
23	Threat Intelligence	5	Elective	UPB

Teaching and assessment methods in the modules can include lectures, tutorials, seminars, exercises, portfolio assignments, project proposals, practical courses, simulations, and other

forms. Assessment details (such as the type of assessment, percentage contribution to the overall module's marks etc.) for each of the modules can be found in the Module Handbook.

Assessment

The D4S Master's Programme provides a flexible, online, modular learning platform tailored to meet the professional needs and preferences of students across Europe. Focusing on essential digital skills— leadership in managing security initiatives, evaluating and mitigating cyber threats, making strategic decisions, and ensuring compliance with legal and regulatory frameworks, the curriculum is aligned with EQF Level 7 standards.

All modules are designed to meet the expectations of EQF Level 7, ensuring that students develop theoretical knowledge, practical skills, and the ability to perform complex professional tasks with a high degree of autonomy and accountability. Thus, they will incorporate two main components as part of their assessment structure:

1) Interactive Technologies: The programme will leverage interactive digital tools such as simulations, virtual labs, and AI-driven analytics to facilitate an engaging and responsive online learning environment.
2) Flexible Learning Paths: Various learning paths will be available, accommodating different learning styles and paces, ensuring that each student can maximize their educational experience according to personal or professional constraints.

Assessment Methods

Each module will employ a variety of assessment methods to evaluate different competencies, including automated quizzes for immediate feedback, peer-assessed assignments to foster collaborative learning, project-based assessments that simulate real-world challenges, among others. However, digital-proctored exams will be mandatory for every module, having a weight over 55% of the final grade and they have to be passed in order to pass the module.

Integrity and Security in Online Assessments

- Authentication and Integrity: Advanced security measures, including secure login procedures and plagiarism detection software, will be implemented to maintain the integrity of assessments.
- User identification: Pairing identity provided in the authentication process and the student itself will be digitally ensured to guarantee that the person taking the exam is the one authenticated.
- Privacy and Data Protection: All assessment activities will strictly comply with GDPR, ensuring that student data is handled with the highest levels of confidentiality and security.

Module Descriptors and Feedback

- Detailed Module descriptors: As part of the Module Handbook, each module is accompanied by a comprehensive descriptor that outlines learning outcomes, detailed assessment criteria, and timelines, all of which are accessible through the online learning platform.
- Feedback: The use of automated tools shall provide students with immediate feedback on quizzes and assignments, allowing for timely adjustments in learning strategies. Furthermore, detailed feedback from instructors will be provided for major assessments, offering personalised insights and guidance to support student development.

Grading System

The Grading Scheme and Honours are outlined in Table 6.

Table 6: Classification of Honours in Relation to Point Average Boundaries

Classification of Master's Degree	Percentage Point Average Boundaries	Description
First-class honours	90%	Achievement includes that required for a Pass and in most respects is significantly and consistently beyond this.
Second-class honours	75%	Achievement includes that required for a Pass and in many respects is significantly beyond this.
Pass	60%	Attains all the minimum intended programme learning outcome.

Resits and Repeat Assessments

If the overall module assessment or examination results in an insufficient grade or the student does not show up on a fixed date or withdraws, the assessment or examination must be repeated in a repeat assessment or resit. Learners can apply for a module repeat assessment in the case of initially failing a module. In such cases, the repeat assessment covers all learning outcomes associated with the failed module. In principle, resits and reassessments of insufficient grades can occur only once during one academic year. If a learner subsequently fails a module after attempting a repeat assessment, it is then necessary for the learner to re-enrol for repeat attendance on the module.

Late Submission of Coursework

Late submission of assignments is only accepted under special circumstances, e.g. illness. The student should inform the lecturer before the deadline of the assignment and should present medical proof on request to the Programme Coordinators team. If not, the lecturer can decide to sanction the student in terms of grading or to refuse the late work. Late submission of an assignment is usually graded with a fail.

To ensure that students with disabilities or special needs receive the necessary support for timely submission of coursework, it is crucial to disclose any disabilities or special needs at the start of the academic year. Delaying disclosure may result in missing out on essential services that assist not only in class participation but also in completing assignments and taking exams. Academic institutions provide specific support services on behalf of the student. Information on the range

of student support services will be rendered available online through the student support services portal on the programme website at https://www.digital4security.eu/support.

External Examiners

External examiners may be invited to jointly assess a sample of project presentations, project/practicum reports, and examination scripts. When multiple evaluators are involved, the final grade is determined either by calculating the average of all scores or by reaching a consensus among the evaluators, depending on the nature of the work and the number of people assessing it.

Academic Misconduct

Plagiarism

Plagiarism occurs when someone uses another person's work, whether text, graphics, tables, photographs, videos, music, or computer code, without proper acknowledgment. This includes failing to use quotation marks for direct quotes, not citing sources for paraphrased work, and not referencing any borrowed material. Additionally, submitting the same work for multiple assignments is also considered plagiarism, which is a serious violation. To avoid plagiarism, it's crucial to properly cite and reference all sources.

Collaboration/Collusion

Where two or more students work together, without the prior authorisation of the course lecturer or supervisor, to produce the same piece of work, and then attempt to present this work as entirely their own work, is also a disciplinary offence.

Poor Scholarship

Poor scholarship may consist of poor referencing, even if there is clearly no intention to deceive. This may be penalised in the mark you receive. Poor scholarship may also consist of very close paraphrasing of published work, or the over-use of long quotations (such that your own contribution is unclear) and will receive a low mark.

Cheating in assessments or examinations

Using, having, sharing, or relying on any unauthorised materials or help during any assessment or academic activity is considered a violation and may lead to disciplinary action.

Outsourcing assessment

Having others complete assessments for oneself whether personally or via any free or commercial service is a disciplinary offence.

Knowingly aiding and abetting academic misconduct

Cases in which students knowingly permit others to copy all or part of their work shall also be subject to the procedures outlined here and considered an offence.

Plagiarism of software code

This policy relates to plagiarism of programming assessments in modules. All assessments and projects are part of the examination process and any attempt to plagiarise is a major offence, punishable accordingly.

Plagiarism includes the following:

- Re-use of code that is based on the learning outcome of the module.
- Submitting another student's work as your own (with or without that person's consent).
- Any act designed to give a student an unfair advantage over another student or the attempt to commit such acts.
- Allowing another student to use your entire program code.
- The reuse of code from previous years' laboratory assessments.
- Not being able to demonstrate an awareness and understanding of the code.
- Taking code with no understanding and not tailored to the requirements of the assessment.
- Re-use of code from other locations that is not substantially modified.

This policy advocates the use of software reuse under strict guidelines namely:

- Each source code program shall contain a standard header which states that this is entirely the authors own work or references the re-used code.

It is the lecturer's discretion to decide if the student is in breach of the above and has plagiarised the software.

Disciplinary Committee

Students found guilty of these offences will be penalised and may be reported to the Master's Board of Directors. The Master's Board of Directors may subsequently convene a Disciplinary Committee. Disciplinary measures include written warnings, suspension from the programme, or expulsion and exclusion of the student from the programme.

Degree, Certification, and Documents

Students who have satisfied all the requirements of the final assessment shall be awarded the Joint Master's degree as per the Cooperation Agreement.

Students who have not satisfied all the requirements of the final assessment within the duration of the degree programme will be required to re-register and pay extension fees.

The degree awarded shall be testified by the issuance of a Master's Degree and Diploma Supplement. The Diploma Supplement shall follow the template developed by the European Commission, the Council of Europe and UNESCO/CEPES and shall be adapted to any further specifications in national legislation where applicable. The Degree Certificate will be issued in the form of a Joint Degree on behalf of the HEIs signatory to the Cooperation Agreement.

Publication and Amendments

These Study and Examination Regulations will be published on the DIGITAL4Security website. Any amendments to these regulations will, after due consultation with the Higher Education Institutions (HEI)s, be confirmed by the Master's Board of Directors in a separate decree. An amendment to these Study and Examination Regulations shall not apply to the current academic cohort unless it may reasonably be assumed that the amendment will not harm the interests of students. In addition, amendments may not influence the following to the detriment of students:

- the degree programme.
- any other decision taken within the meaning of these regulations concerning a student.

Digital4Security

Shaping Europe's cyber future

Teaching Faculty CVs

Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty

Table of Contents

Overview

This document is the consolidation of detailed CVs of the teaching faculty for the Digital4Security Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty.

Polytechnic University of Bucharest

Name	*Costin Carabaș*		
Post	*Teaching assistant,* *Teaching: Blockchain Protocols and Distributed Applications, Operating Systems* *Faculty of Automatic Control and Computer Science* *Polytechnic University of Bucharest*		
Academic career	*Teaching assistant (CS)* *Doctoral degree (CS)* *Graduate degree (CS)* *Undergraduate degree (CS)*	*Polytechnic University of Bucharest*	*2022-present* *2021* *2016* *2014*
Employment	*Teaching Assistant* *Research Assistant* *Software Engineer* *Software Engineer*	*Polytechnic University of Bucharest* *Polytechnic University of Bucharest* *NXP Semiconductors* *Intel Corporation*	*2022-present* *2018-2022* *2017-2018* *2013-2016*
Research and development projects over the last 5 years	*Name of project or research focus:* Improving the Security of Blockchain Protocols and Applications *Period and any other information: 2023-2024* *Amount of financing: 10.000 EUR* *Name of project or research focus:* Documents in the Air *Period and any other information: 2020-2022* *Amount of financing: 100.000 EUR* *Name of project or research focus:* ATLAS *Period and any other information: 2018-2021* *Amount of financing: 300.000 EUR*		
Industry collaborations over the last 5 years	*MultiversX Blockchain*		

Patents and proprietary rights	*N\A*
Important publications over the last 5 years	https://scholar.google.ro/citations?user=KFEUaUwAAAAJ&hl=en
Activities in specialist bodies over the last 5 years	*N\A*

Name	*Radu Mantu*		
Post	*Research assistant,* *Teaching: Intro to Cybersecurity, Performance Evaluation* *Faculty of Automatic Control and Computer Science* *Polytechnic University of Bucharest*		
Academic career	*Research assistant (CS)* *Doctoral degree (CS)* *Graduate degree (CS)* *Undergraduate degree (CS)*	*Polytechnic University of Bucharest*	*2020-present* *2024 (expected)* *2020* *2018*
Employment	*Research Assistant* *Software Engineer* *Research Assistant* *Research Intern* *SRE Intern*	*Polytechnic University of Bucharest* *Sanctuary Systems GmbH.* *Technische Universität Darmstadt* *National University of Singapore* *Fitbit*	*2020-present* *2023-present* *2022* *2020* *2018*
Research and development projects over the last 5 years	*Secure channel between io and trusted processing unit: intel software guard extension (PN-III-P2-2.1-PTE-2019-0802), 2020-2022*		

	Avant-garde technology hub for advanced security (PN-III-P1-1.2-PCCDI-2017-0272), 2018-2021
Industry collaborations over the last 5 years	*N\A*
Patents and proprietary rights	*N\A*
Important publications over the last 5 years	*https://scholar.google.com/citations?user=4m1APEQAAAAJ*
Activities in specialist bodies over the last 5 years	*N\A*

Name	*Adrian-Răzvan Deaconescu*		
Post	*Associate Professor* *Teaching Operating Systems, Software Security, and Mobile Security Classes*		
Academic career	*Doctorate (CS)* *Undergraduate degree (CS)*	*POLITEHINCA Bucharest* *POLITEHINICA Bucharest*	*2011* *2006*
Employment	*Associate Professor* *Assistant Professor* *Teaching Assistant*	*POLITEHNICA Bucharest* *POLITEHNICA Bucharest* *POLITEHNICA Bucharest*	*2019-present* *2012-2019* *2006-2012*
Research and development	*Intelligence and Cybersecurity in Europe Joint Master*		

projects over the last 5 years	*November 2022-January 2024* *3iL France, Hennalux* *55.000 EUR* *SASHA: Platform for Security Assessment of Smart Home Interconnected Applications PN III (2013-2020) / PED 2019, Proiect PN-III-P2-2.1-PED-2019-5392* *November 2020 - October 2022* *70.000 EUR* *Using the Open Source Collaborative Model for the Development, Delivery and Curation of Digital Educational Content* *Granturi SEE 2014-2020, contract 21-COP-0016* *April 2022-September 2023* *158.444 EUR* *UNICORE, H2020-EU.2.1.1, Grant agreement ID: 825377* *IBM Israel – Science And Technology Ltd., NEC Laboratories Europe GmbH, Ecole Polytechnique Fédérale de Lausanne, Consorci de Serveis Universitaris de Catalunya, Université de Liège, Accelleran, Vrije Universiteit Amsterdam, Nextworks, Ekinops, Orange Romania, S.C. Correct Networks S.R.L.* *January 2019 – December 2021*

	CloudPrecis, Programul Operațional Competitivitate 2014-2020, MySmis cod: 124812 *November 2021-October 2023*
Industry collaborations over the last 5 years	*Technical Contributions to the Unikraft Project, 1480/27.0.2021* *NEC Laboratories Europe GmbH* *60.000 EUR* *February 1, 2021 – December 31, 2021*
Patents and proprietary rights	-
Important publications over the last 5 years	*https://scholar.google.com/citations?user=1xehMdQAAAAJ&hl=en*
Activities in specialist bodies over the last 5 years	-

National College of Ireland

Name	*Michael Bradford*		
Post	*Assistant Professor (National College of Ireland / School of Computing)* *Programme Director MSc in Data Analytics*		
Academic career	*MSc in Mathematics* BSc (Hons) in Mathematics *Diploma in Information Systems* *BSc*	*UCD(NUI)* *DIT* *TCD* *UCD(NUI)*	*2009* *2008* *2000* *1995*
Employment	*Position* *Assistant Professor.* *IT Development Manager* *Senior Software Developer* *Software Developer*	*Employer* *National College of Ireland* *Financial Sector*	*Period* *Jan 2010 –* *2002 – 2008* *1998 - 2002* *1995 - 1998*
Research and development projects over the last 5 years			
Industry collaborations over the last 5 years			
Patents and proprietary rights	*Title*		*Year*
Important publications over the last 5 years	*Please link your research gate profile or any other official website that lists your publications.* *Alba González-Cebrián, Luke A. McGuinness, Michael Bradford, Adriana E. Chis, Horacio González-Vélez: Automatic Versioning of Time Series Datasets: a FAIR Algorithmic Approach. e-Science 2022: 204-213.* *Cristina Hava Muntean, Nour El Mawas, Michael Bradford, Pramod Pathak: Investigating the Impact of an Immersive Computer-*		

	based Math Game on the Learning Process of Undergraduate Students. FIE 2018: 1-8 *Michael Bradford, Cristina Hava Muntean, Pramod Pathak: An analysis of flip-classroom pedagogy in first year undergraduate mathematics for computing. FIE 2014: 1-5*
Activities in specialist bodies over the last 5 years	*Organisation* *Role* *Period*

German University of Digital Science

Name	**Dr. Pejman Najafi**		
Post	Lecturer, Cybersecurity Modules Instructor at the German University of Digital Science (UDS), Potsdam, Germany		
Academic career	**Current Academic Appointment**: Lecturer	German University of Digital Science, Potsdam, Germany	Oct 2024 – present
	Doctorate (Cybersecurity) PhD Thesis: Leveraging Data Science & Engineering for Advanced Security Operations	Hasso Plattner Institute, Potsdam, Germany	Aug 2016 – Sep 2023
	Graduate Degree (MSc Information Security with International Research)	University College London, UK	Sep 2013 – Dec 2015
	Undergraduate Degree (BEng Electronic, Computer Engineering)	Queen Mary University of London, UK	Sep 2010 – July 2013
Employment	Lecturer; Main Instructor for a 5 ECTS course: Cybersecurity Fundamentals; Responsible for M.Sc. Cybersecurity topic: AI & Emerging Topics in Cybersecurity	German University of Digital Science (UDS), Potsdam, Germany	2024 – Present
	Postdoctoral Researcher; AI-driven Security Operations, Advanced Threat Detection, Alert Management	Hasso Plattner Institute, Potsdam, Germany	Jun 2023 – Present

	Senior Data Scientist/Engineer (Remote Contractor); Data science and engineering for SOCs, statistical analysis, anomaly detection, alert correlation, and AI/LLM-assisted alert monitoring	Shell Global, The Hague, Netherlands	Jun 2019 – Present
	Ph.D. Researcher; Big Data Architectures, Machine Learning, SIEM, Threat Intelligence	Hasso Plattner Institute, Potsdam, Germany	Aug 2016 – Jun 2023
Research and development projects over the last 5 years	**Project**: Threat Intelligence Platform Period: Jan 2018 – Present Research Focus: Building a platform for threat intelligence ingestion and OSINT analysis. Partners: Bundesdruckerei (Germany), Hasso Plattner Institute (Potsdam, Germany) **Project**: Next-Gen SIEM Period: Feb 2017 – Present Research Focus: Development of a scalable, unified platform for security data processing and analysis. Partners: T-System (Germany), Hasso Plattner Institute (Potsdam, Germany)		
Industry collaborations over the last 5 years	**Project**: Data Science Applications in Security Operations Partner: Shell Global, The Hague, Netherlands Period: 2019 – Present Focus: SIEM-based data analytics, alert correlation, advanced threat detection. **Project**: Research on Attack Graphs and Knowledge Graphs Partner: Deutsche Telekom AG, T-Labs Period: Aug 2020 – Dec 2020 Focus: Using graphs to model infrastructures, policies, and event logs. **Project**: High-Performance Big Data Pipelines Partner: SAP, Germany		

	Period: Nov 2016 – Dec 2021 Focus: Log monitoring and data analytics for SAP services.
Important publications over the last 5 years	Research Gate: https://www.researchgate.net/profile/Pejman-Najafi Google Scholar: https://scholar.google.de/citations?hl=en&user=Ey7CtREAAAAJ HEOD: Human-assisted Ensemble Outlier Detection for cybersecurity; Pejman Najafi, Feng Cheng, Christoph Meinel; Computers & Security 146 (2024): 104040 You are your friends: Detecting malware via guilt-by-association and exempt-by-reputation; Pejman Najafi, Wenzel Puenter, Feng Cheng, Christoph Meinel; Computers & Security 136 (2024): 103519 SIEMA: Bringing Advanced Analytics to Legacy Security Information and Event Management; Pejman Najafi, Feng Cheng, Christoph Meinel; International Conference on Security and Privacy in Communication Systems; (2021) Large language models in cybersecurity: State-of-the-art; FN Motlagh, M Hajizadeh, M Majd, P Najafi MalRank: A Measure of Maliciousness in SIEM-based Knowledge Graphs; Pejman Najafi, Alexander Muehle, Wenzel Puenter, Feng Cheng, and Christoph Meinel; Proceedings of the 35th Annual Computer Security Applications Conference. 2019 NLP-based Entity Behavior Analytics for Malware Detection; Pejman Najaf, Daniel Koehler, Feng Cheng, Christoph Meinel; 2021 IEEE International Performance, Computing, and Communications Conference (IPCCC). IEEE, 2021. Detect Me If You Can: Spam Bot Detection Using Inductive Representation Learning; S Ali Alhosseini, R Bin Tareaf, P Najafi, C Meinel; Companion Proceedings of The 2019 World Wide Web Conference

Activities in specialist bodies over the last 5 years	Hasso Plattner Institute, Potsdam, Germany	Teaching Assistant for multiple courses, including Big Data Security Analytics and Network Security in Practice	2017 – Present
	Hasso Plattner Institute, Potsdam, Germany	Dedicated Server Room Administrator; Managed server setup and configuration, hardware, and software maintenance.	Mar 2018 – Aug 2024

University of Rijeka

Name	*Prof. Marina Ivasic-Kos, PhD*		
Post	*- Teaching on postgraduate, graduate and Doctoral Studies at the Faculty of Informatics and Digital technologies, University of Rijeka in the field of Computer Science and Artificial Intelligence (Fundamentals of Computer Game Development, Programming paradigms, Intelligent systems, Machine and Deep Learning, Soft Computing, Computer Vision, Computer Vision and Image processing and Pattern Analysis)*		
Academic career	*Full Professor, Head of the Laboratory*	*University of Rijeka*	*2023*
	Associate Professor, Dean		*2020*
	Associate Professor, Head of the Laboratory	*University of Rijeka*	*2018*
	Assistant professor	*University of Rijeka*	*2013*
	Assistant, PhD Degree (Computer Science, Artificial Intelligence, Computer Vision, Soft Computing)	*University of Rijeka*	*2012*
	Assistant, M.Sc. Degree in Information Science (Software engineering, Databases)	*University of Zagreb*	*2001*
	M. S. Degree (Mathematics and Computer science)	*University of Zagreb*	*1997*
		University of Rijeka	
Employment	*Full professor* *- Head of Laboratory for Pattern Recognition and Soft Computing*	*Faculty of Informatics and Digital technologies*	*2023 –*

	- Head of the Laboratory for Computer Vision, Virtual and Augmented Reality	*University of Rijeka* *Centre for Artificial Intelligence and Cybersecurity, University of Rijeka*
Research and development projects over the last 5 years	• ***SAR-DAG: Automatic detection and geolocation of persons recorded by a drone in search and rescue operations,*** *University of Rijeka, uniri-iskusni-drustv-23-278, 2024-2025, project leader and principal investigator* • ***DIGITAL4Security – European Masters Programme in Cybersecurity Management & Data Sovereignty, 101123430, DIGITAL EU Horizon,*** *2023.-2027., partner leader* • *Horizon* ***INNO2MARE, Strengthening the capacity for excellence of Slovenian and Croatian innovation ecosystems to support the digital and green transitions of maritime regions****, HORIZON-WIDERA-2022-ACCESS-04, 2022.-2026., partner leader and WP3, T3.3 leader* • ***Image-based AI-assisted diagnostics of canine ocular disease - AICODD****, Animal Eye Consultants of Iowa, Iowa, USA, 2022.-2025, project leader and principal investigator* • ***EDIH Adria****, European Digital Innovation Hub Adriatic Croatia, DIGITAL-2021-EDIH-01, 2023.-2025., WP3 leader* • *HRZZ research project* ***IP-2016-06-8345, Automatic recognition of actions and activities in the multimedia content of the sport domain - RAASS*** *(2017-2020) - project leader and principal investigator* • **Automatic recognition of sports techniques for young athletes and recreationalists for the purpose of adopting motor skills and enhancement of style**, uniri-drustv-18-222, University of Rijeka, 2019-2021, project leader and principal investigator • *HRZZ research project* ***KACAVIS: knowledge-based approach for analysis of a multitude of people in supervisory systems****, head of prof. Ph.D. S Ribarić, HRZZ-IP-2018, 2018-2021. – research associate*	
Industry collaborations over the last 5 years	*Project title* *Partners*	
Patents and proprietary rights	*Title*	*Year*

Important publications over the last 5 years	• *Buric, Matija, Grozdanic, Sinisa, Ivasic-Kos, Marina, Diagnosis of ophthalmologic diseases in canines based on images using neural networks for image segmentation, Elsevier Heliyon, v. 10(19), pp. 2405-8440, 2024, Q1 Scopus.* • *A. Vorkapic, M. Pobar, and M. Ivasic-Kos.* ***"A computer vision approach to estimate the localized sea state." Ocean Engineering*** *309 (2024): 118318, Q1 Wos, Scopus.* • *G. Paulin, S. Sambolek and M. Ivasic-Kos,* ***Application of Raycast Method for Person Geolocalization and Distance Determination Using UAV Images in Real-World Land Search and Rescue Scenarios. Expert systems with applications****, (2023), Q1 Wos, Scopus.* • *G. Paulin and M. Ivasic-Kos,* ***Review and analysis of synthetic dataset generation methods and techniques for application in computer vision****. Artificial Intelligence Review 56, 9221–9265 (2023)., Q1 Scopus, WoS.* • *R. Sajina and M. Ivasic-Kos,* ***MPFSIR: An Effective Multi-Person Pose Forecasting Model with Social Interaction Recognition,*** *IEEE Access, vol. 11, pp. 84822-84833, 2023, Q1 Scopus, Wos* • *K. Host, M. Pobar, and M. Ivasic-Kos, "****Analysis of Movement and Activities of Handball Players Using Deep Neural Networks****," Journal of Imaging, vol. 9, no. 4, p. 80, 2023., Q2 Scopus.* • *F. Matkovic, M. Ivasic-Kos and S. Ribaric. (2022).* ***A new approach to dominant motion pattern recognition at the macroscopic crowd level****. Engineering Applications of Artificial Intelligence, 116, 105387, Q1 Scopus, WoS.* • *B. Gasparovic, L. Lerga, G. Mausa and M. Ivasic-Kos. (2022).* ***Deep Learning Approach for Objects Detection in Underwater Pipeline Images****. Applied Artificial Intelligence, 36(1), 2146853., Q3 Scopus, Q2 WoS.* • *K. Host and M. Ivasic.-Kos (2022).* ***An overview of Human Action Recognition in sports based on Computer Vision****. Heliyon, Q1 Scopus, Q2 WoS.* • *R. Sajina and M. Ivasic-Kos, (2022).* ***3D Pose Estimation and Tracking in Handball Actions Using a Monocular Camera****. Journal of Imaging, 8(11), 308, Q2 Scopus* • *S. Sambolek, M. Ivasic-Kos,* ***Automatic Person Detection in Search and Rescue***

	***Operations Using Deep CNN Detectors**, IEEE Access 9, 37905-37922, 2021, Q1 Scopus, WoS.* • *M. Kristo, M. Pobar, and M. Ivasic-Kos; **Thermal Object Detection in Difficult Weather Conditions Using YOLO**, IEEE Access, Vol. 8, 125459 - 125476, 2020, Q1 Scopus, WoS* • *M. Pobar and M. Ivasic-Kos. **Active Player Detection in Handball Scenes Based on Activity Measures** // Sensors, 20 (2020), 5; 1475, 24, doi:10.3390/s20051475, IF 3.03, Q1 Scopus, WoS*
Activities in specialist bodies over the last 5 years	*Organisation Role Period* *Membership without a specific role need not be mentioned* • *Expert for the **European Health and Digital Executive Agency (HADEA)** for the competition **DIGITAL-2023-SKILLS-05**, 2024* • *Expert for the **European Research Executive Agency (REA)** and reviewed projects submitted to the competition **HORIZON-WIDERA-2023-ACCESS-02,** 2023* • *Reviewer and member of the Panel for evaluation of scientific projects submitted to the competition YUFE - Young Universities for the Future of Europe, Postdoc program **Citizens' well-being**, EU, 2022* • *Reviewer and member of the Panel for the evaluation of projects submitted to the Croatian Science Foundation Program for Cooperation with Croatian Scientists in the Diaspora ("**Scientific Cooperation**"), 2019, 2020*

Name	*Prof. dr.sc. Sanda Martinčić-Ipšić*		
Post	*Professor, courses in natural language processing, data mining, data engineering, artificial intelligence, MLOPS* *Faculty of Informatics and Digital technologies* *University of Rijeka*		
Academic career	*Assistant professor* *Doctorate (Artificial Intelligence- automatic speech recognition and speech synthesis)* *Undergraduate degree (Computer science)*	*University of Rijeka* *University of Zagreb* *University of Ljubljana*	*2009* *2007* *1994*

Employment	*Full professor with tenure* *University of Rijeka* *2024 -*
Research and development projects over the last 5 years	*Digital4Security, Digital4Security– European Masters Programme in Cybersecurity, Management & Data Sovereignty, DIGITAL-2022-SKILLS-03, 2023 - 2026.* *EDIH Adria, Digital Europe, WP3: Task 3.4. Internal competence building, task* *3.4. leader, 2023 - 2026.* *H2020 MESOC Measuring the Social Dimension of Culture, 2020 - 2023.* *HRZZ Multilayer Framework for the Information Spreading Characterization in* *Social Media during the COVID-19 Crisis InfoCoV, 2020 - 2022.* *Advisory Board H2020 Easy Rights - Inclusive Future for All: Enabling Immigrants to Easily Know and Exercise their Rights easyRights, 2021 - 2022.* *Management Committee Member* *COST Action CA18231 - Multi3Generation: Multi-task, Multilingual, Multi-modal* *Language Generation, Multi3Generation, 2019 - 2023.* *ICT COST Action CA15109: "European Cooperation for Statistics of Network Data* *Science", COSTNET, 2016 - 2020.*
Industry collaborations over the last 5 years	*Project title* *Partners*
Patents and proprietary rights	*Title* *Year*
Important publications over the last 5 years	*Vorkapić, A.; Martinčić-Ipšić, S.; Piltaver, R. Interpretable Machine Learning: A Case Study on Predicting Fuel Consumption in VLGC Ship Propulsion. Journal of Marine Science and Engineering (JMSE), 2024, 12(10), 1849. https://doi.org/10.3390/jmse12101849. (WOS SCIE Q1, IF 2.7 SJR Q2)*

	E. Erdem et al. Neural Natural Language Generation: A Survey on Multilinguality, Multimodality, Controllability and Learning, Journal of Artificial Intelligence Research (JAIR)), https://doi.org/10.1613/jair.1.12918 Vol. 73. 2022. (WOS SCIE Q2, IF 3.635, SJR Q2) *S. Beliga, S. Martinčić-Ipšić, M. Matešić, I. Petrijevčanin Vuksanović, A. Meštrović. Infoveillance of the Croatian Online Media During the COVID -19 Pandemic: A One-Year Longitudinal Study Using Natural Language Processing JMIR Public Health and Surveillance, 7(12): 31540, 2021. 10.2196/31540 (WOS Q1, IF 14.557)* *K. Babić, M. Petrović, S. Beliga, S. Martinčić-Ipšić, M.Matešić, A. Meštrović. Characterisation of COVID-19-Related Tweets in the Croatian Language: Framework Based on the Cro-CoV-cseBERT Model. Applied Sciences, 11, 10442. 2021. https://doi.org/10.3390/app112110442 (WOS Q2, IF 2.838, Scopus Q2 SJR 0.435)* *A. Vorkapić, R. Radonja, S. Martinčić-Ipšić. Predicting Seagoing Ship Energy Efficiency from the Operational Data, Sensors, Vol 21, 2832 2021. https://doi.org/10.3390/s21082832 (WOS SCIE Q1, IF 3.847)* *K. Babić, S. Martinčić-Ipšić, A. Meštrović. Survey of Neural Text Representation Models. Information, Vol. 11, 511, 2020. doi:10.3390/info11110511 (WOS Emerging Sources IF 0.52 Q3, SJR Q3)* *Đ. Vukić, S. Martinčić-Ipšić, A. Meštrović. "Structural Analysis of Factual, Conceptual, Procedural, and Metacognitive Knowledge in a Multidimensional Knowledge Network". Complexity, pp. 1-17, 2020. https://doi.org/10.1155/2020/9407162 (WOS SCIE Q2, IF 2.833, SJR Q1)* *S. Martinčić-Ipšić, T. Miličić, Lj. Todorovski. "The Influence of Feature Representation of Text on the Performance of Document Classification". Applied Sciences, Vol. 9, No. 4, pp. 743-770, 2019. (IF 2.474, Q2)*
Activities in specialist bodies over the last 5 years	*Organisation* *Role* *Period* *Membership without a specific role need not be mentioned*

Name	*Tomislav Slaviček-Car*		
Post	*Teaching assistent*		
Academic career	*Initial academic appointment* *Graduate degree* *Undergraduate degree*	*University of Rijeka* *University of Rijeka* *University of Rijeka*	*2023* *2017* *2014*
Employment	*Teaching assistant* *CEO* *Data Science Manager* *Data Science Lead* *Data Science Analyst*	*University of Rijeka* *Tech-Art* *Ancora.ai* *Ancora.ai* *Ancora.ai*	*10/2023-current* *4/2021-10/2023* *6/2019 - 12/2020* *3/2018 - 6/2019* *11/2017 – 3/2018*
Research and development projects over the last 5 years			
Industry collaborations over the last 5 years	*Safe Online* *Ancora.ai*		

University of Brescia

Name	*Fabrizio Corona*
Post	*Legal Informatics*

Academic career	*Research Fellow* *Social Sciences and Humanities" XXXV Ciclo - Curriculum "Law, Psychology and Education"*	*University of Brescia* *University Niccolò Cusano*	*2024* *2023*
Employment	*Research Fellow* *Lawyer*	*University of Brescia* *COA Naples*	*2024* *2022*
Research and development projects over the last 5 years	*Digital4Security – European Masters Programme in Cybersecurity Management & Data Sovereignty, research fellow, 2024* *SCAN - Small Claims Analysis Net ott 2018 - gen 2021, participant contact* *CREA - Conflict Resolution With Equitative Algorithm set 2017 - set 2019, research fellow and coordinator contact*		
Industry collaborations over the last 5 years	*n/a*		
Patents and proprietary rights	*n/a*		
Important publications over the last 5 years	Book Chapters • 2024, CORONA F. IA e Giustizia. In (a cura di IASELLI M,), AI ACT: Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024 Maggioli Editore; • 2023, CORONA F. I reati informatici. In (a cura di IASELLI M. CARIA G.B., Cybersecurity & Cyberwarfare, diritto, tecnologia e sicurezza, EPC Editore 9788892881945 • 2022, CORONA F. La privacy dei minori online: dagli strumenti self-regulation dell'Unione Europea alle tutele previste dal GDPR. In (a cura di) FODERARO A., PALUMBO P., Diritti e tutela dei minori profili interdisciplinari, Editoriale Scientifica. ISBN: 9791259764584 • 2022, DE LUCA PICIONE, R., MARTINI, E., CORONA, F., FALZARANO, M. L., & CICCHELLA, S. (2022). Bullying and Cyber-Bullying: A Dialogue Between Psychology, Sociology, and Law to Understand and to Counteract Youth Violence. In MARCHISIO E. (a cura di), Handbook of Research on Applying Emerging Technologies Across Multiple Disciplines. IGI Global. ISBN: 9781799884767 • 2021, DEL PIZZO A., CORONA F. Contact tracing: criticità e questioni aperte sul trattamento del dato. In (a cura di) D'AMBROSIO I., PALUMBO P., Diritto, economia e società		

	dopo la pandemia, Editoriale Scientifica. ISBN: 979-12-5976-158-3 (materiale in studio) • 2021, CORONA F. Le attività di digital forensics nel cybercrime. In: (a cura di): CORONA F., Reati informatici e investigazioni digitali. Diffamazione via web - Prove digitali - Sex crimes - Cyberstalking - Cyberbullismo - Reati privacy. Pacini Giuridica. ISBN: 978-88-3379-368-9 • 2021, CORONA F. Il trattamento della prova digitale nel cybercrime. In: (a cura di): CORONA F., Reati informatici e investigazioni digitali. Diffamazione via web - Prove digitali - Sex crimes - Cyberstalking - Cyberbullismo - Reati privacy. Pacini Giuridica. ISBN: 978-88-3379-368-9 • 2021, CORONA F. Il cybercrime: soggetto, oggetto e condotta. In: (a cura di): CORONA F., Reati informatici e investigazioni digitali. Diffamazione via web - Prove digitali - Sex crimes - Cyberstalking - Cyberbullismo - Reati privacy. Pacini Giuridica. ISBN: 978-88-3379-368-9 • 2021, CORONA F. I reati informatici tradizionali. In: (a cura di): IASELLI M., CORONA F., Manuale di diritto di internet. Le principali ed innovative tematiche dell'informatica giuridica: l'ambito civile, penale, amministrativo e le tecnologie emergenti. EPC Editore, ISBN: 978-88-9288-042-9 • 2021, CORONA F. Le ODR e l'Intelligenza Artificiale. In: (a cura di): IASELLI M., CORONA F., Manuale di diritto di internet. Le principali ed innovative tematiche dell'informatica giuridica: l'ambito civile, penale, amministrativo e le tecnologie emergenti. EPC Editore, ISBN: 978-88-9288-042-9 • 2021, CORONA F. Il deepweb ed il darkweb. In: (a cura di): IASELLI M., CORONA F., Manuale di diritto di internet. Le principali ed innovative tematiche dell'informatica giuridica: l'ambito civile, penale, amministrativo e le tecnologie emergenti. EPC Editore, ISBN: 978-88-9288-042-9 • 2021, CORONA F. I contratti informatici. In: (a cura di): IASELLI M., CORONA F., Manuale di diritto di internet. Le principali ed innovative tematiche dell'informatica giuridica: l'ambito civile, penale, amministrativo e le tecnologie emergenti. EPC Editore, ISBN: 978-88-9288-042-9 • 2021, CORONA F La Successione nel patrimonio digitale. In: (a cura di): IASELLI M., CORONA F., Manuale di diritto di internet. Le principali ed innovative tematiche dell'informatica giuridica: l'ambito civile, penale, amministrativo e le tecnologie emergenti. EPC Editore, ISBN: 978-88-9288-042-9 • 2020, GIACALONE M. CORONA F. CREA – Conflict Resolution with Equitative Algorithms: a Cloud Based Decision Spport System. In: (a cura di): AMATO F; ROMEO F; CORONA F., Algorithmic Conflict Resolution – The CREA platform. Napoli: Editoriale Scientifica, ISBN: 978-88-9391-627-1

	• 2020, AMATO F., CORONA F. The Platform Specification. In: (a cura di): AMATO F; ROMEO F; CORONA F., Algorithmic Conflict Resolution – The CREA platform. Napoli: Editoriale Scientifica, ISBN: 978-88-9391-627-1 • 2020, IASELLI M., CORONA F. I contratti online. In A.DI AMATO (a cura di), I contratti di Impresa. Giuffrè 2020 ISBN: 978-88-2881937-0; • 2020, IASELLI M., CORONA F. I contratti informatici. In A.DI AMATO (a cura di), I contratti di Impresa. Giuffrè 2020 ISBN: 978-88-2881937-0; • 2020, CORONA F. Le figure soggettive della privacy. In M.IASELLI (a cura di), Formulario Privacy - Atti completi relativi ai principali istituti previsti dal Reg. UE 2016/679 e dal d.gls. 196/2003. Giuffré 2020 ISBN: 978-88-82882261-5 • 2020, CORONA F. La contitolarità al trattamento. In M.IASELLI (a cura di), Formulario Privacy - Atti completi relativi ai principali istituti previsti dal Reg. UE 2016/679 e dal d.gls. 196/2003. Giuffré 2020 ISBN: 978-88-82882261-5 • 2020, CORONA F. Il responsabile del trattamento. In M.IASELLI (a cura di), Formulario Privacy - Atti completi relativi ai principali istituti previsti dal Reg. UE 2016/679 e dal d.gls. 196/2003. Giuffré 2020 ISBN: 978-88-82882261-5 • 2020, CORONA F. Il regolamento informatico. In M.IASELLI (a cura di), Formulario Privacy - Atti completi relativi ai principali istituti previsti dal Reg. UE 2016/679 e dal d.gls. 196/2003. Giuffré 2020 ISBN: 978-88-82882261-5 • 2020, CORONA F. Il cyberbullismo. In: M.IASELLI (a cura di), Investigazioni digitali. Giuffré Francis Lefebvre ISBN: 978-88-2882394-0; • 2020, CORONA F. Il contratto di cloud computing. In M.IASELLI (a cura di), Formulario Privacy - Atti completi relativi ai principali istituti previsti dal Reg. UE 2016/679 e dal d.gls. 196/2003. Giuffré 2020 ISBN: 978-88-82882261-5 • 2020, CORONA F. I reati informatici. In F.CELENTANO (a cura di), Manuale breve di informatica del giurista - seconda edizione, Pacini Editore, ISBN: 978-88-3379-265-1 **Article** • CORONA F. (2024) L'evoluzione del processo decisionale tra giudizio automatico e sostituzione giudiziaria, L'Ircocervo, p.175-193 • CORONA F (2023). La decisione del Giudice tra precedente giudiziale e predizione artificiale. DEMOCRAZIA E DIRITTI SOCIALI, p. 1-16, ISSN: 2610-9166 • 2022 CORONA F. La tutela del patrimonio digitale oltre la vita. Nomos le attualità nel diritto n. 1/2022, ISSN: 2279-7238 • 2020, CORONA F. DEL PIZZO A. Cervelli elettronici al servizio della giustizia. Nomos le attualità nel diritto n. 3/2020, ISSN: 2279-7238 • 2020, DEL PIZZO A. – CORONA F. " Diffusione COVID-19: il trade off tra contact tracing e trattamento dei dati

	personali degli individui", in Diritto di Internet n.4/2020. ISSN:2612-4491 (scansione studio) • 2020, CORONA F., "E-demogracy fra sviluppo delle tecnologie e processi partecipativi", Cammino Diritto n.9/2020. ISSN: 2532-9871 • 2019, ROMEO F., DI STASIO G., GIACALONE M., CORONA F., SACCO F.G., "The Small Claims Analysis Net Project". Jusletter IT. ISSN: 1664-848X • 2019, CORONA F., GIACALONE M., " L'evoluzione storica delle odr: dall'emoticon ai sistemi di fair division", I-lex, Fascicolo 12, 1-3. ISSN 1825-1927 • 2020, CORONA F., DEL PIZZO A., " Giustizia elettronica: può l'elaboratore sostituire il giudice?", I-lex, Fascicolo 13, 1. ISSN 1825-1927 • 2019, CORONA F., DALL'AGLIO M., MORELLI G., "The application of fair division systems in cases involving the judicial division of assets. Jusletter IT. ISSN: 1664-848X **Book** • CORONA F (2023). Giustizia Predittiva. Quando gli algoritmi pervadono il diritto. p. 1-172, ISBN: 9791221807158
Activities in specialist bodies over the last 5 years	*Member of the Expert Pool in support of the European Data Protection Board (EDPB). The European Data Protection Board (EDPB), 2022 - today*

Name	*Susanna Pozzolo*		
Post	*Philosophy of Law / Legal Informatics*		
Academic career	*Full Professor* Associate Professor *Researcher* *Undergraduate degree (subject)*	*University of Brescia* *University of Brescia* *University of Brescia* *Institution*	*2021* *2015* *2005* *Year*
Employment	*Full Professor*	*University of Brescia*	*2021 - Today*

Research and development projects over the last 5 years	*Horizon 2020 Marie Sklodowska Curie project involves secondment in partner institutions- periods held at Afadis, Universidad Complutense, Madrid:.from 26/11/19 to 25/02/20; from 29/09/2019 to 4/12/2019 (with some certified breaks), from 11/01/ 2018 to 10/02/2018* *Digital4Security (DIGITAL-2022-SKILLS-03-SPECIALISED-EDU) Unit Manager Budget-It: Building Gender Equality through gender budgeting for Institutional Transformation (HORIZON-WIDERA-2022-ERA-01 Unit Manager* *Inclusion4All: Trans, Intersex and Nonbinary People at Work Role performed: researcher; Budget: € 311,543.34* *School's OUT, Role performed: researcher Budget: € 312,152.17 UniDiversity: Universities toward Diversities Role played: researcher Budget: € 311,147.00 - Academic partners: Panteion University (Greece), Vytautas Magnus University (Lithuania)* *LetsGoByTalking - Protecting and defending the rights of victims of anti- LGBT hate crimes Role performed: Researcher; Budget: € 630,604.50 - Academic partners: Universitat de Barcelona (Spain), Universitat de Girona (Spain), Uniwersytet Wroclawski (Poland)* *OPENDOORS - Promoting Inclusive and Competent Health Care for LGBTI People. Role performed: researcher; Budget: € 312,351.19 - Academic partners: Universitat de Girona (E)* *RISE Women with Disabilities In Social Engagement (RISEWISE) Role played: Scientific manager of the UNIBS Unit. Budget: €1,809,000.00 - Academic partners: Universidade do Minho (Portugal), Universidad Complutense de Madrid (Spain), Middle East Technical University (Turkey), Stockholm University (Sweden), University of Genoa (Italy), University of Ljubljana (Slovenia)* *Call It Hate: Raising Awareness on Anti-LGBT Hate Crime Role performed: Scientific project manager; Budget: € 1,034,496.79 - Academic Partners: University of Ljubljana (Slovenia)*

	Systemic Action for Gender Equality (SAGE) Role performed: Scientific manager of UNIBS unit; Budget: € 2,276,853.75 - Academic partners: Trinity College Dublin (Ireland), Instituto Universitário De Lisboa (Portugal), International University of Sarajevo (Bosnia), Kadir Has University (Turkey), Sciences Po Bordeaux (France), Queen's University Belfast (UK) - RTDA funded
Industry collaborations over the last 5 years	*N/A*
Patents and proprietary rights	*N/A*
Important publications over the last 5 years	***Journal Articles*** *1. Somos cuerpos. Politicas de los cuerpos y maternidad, In Atlánticas. Revista Internacional de Estudio Feministas, 2, V0L 8, 2023, PP. 55-78.* *2. Oltre le gerarchie, la societa, in Rivista di Politeia 2, 2023, PP.64-67.* *3. Introduzione. Giustizia riparativa: una definizione in via di costruzione. Maria Giovanna Foddai e Michelina Masia In RAGION PRATICA vol. 59, 2022* *4. Introduzione. Dalla istituzionalizzazione della critica di genere alla costruzione di una societa inclusiva: questioni e sfide per la filosofia del diritto. Con, Thomas Casadei, Orsetta Giolo, Lucia Re, in RIVISTA DI FILOSOFIA DEL DIRITTO vol. 2, 2022* *5. (con G. Viggiani) Come gamberi spaventati. Un balzo indietro di cent ' anni nell ' affermazione dell ' uguaglianza e dei diritti delle donne, Questione giustizia, 4/2022, pp. 134-148. 1972-5531* *6. Moreso, un punto de vista interno y la defensa de un mundo que nos gustaria bien ordendado. Breves comentarios a unos capitulos de Lo normativo. Comentario a Jose Juan Moreso, Lo normativo: viariedades y variaciones, «Eunonia», 22, 2022, pp. 518-533* *7. No hay Humanidad sin Mujeres, Direito Publico, 18, 98, 2021. 10.11117/rdp.v18i98.5852*

	8. Locatio ventris. Il corpo come mezzo e come fine, ≪Ragion pratica≫, 1/2021, pp. 161-191. (A) *9. Some Observation on the Standard Balancing Theory, in ≪Rivista di filosofia del diritto≫, 2020, pp. 315- 332 (ISSN 2280-482X) - fascia A* *10. Un equilibrio forse instabile. Diritti delle minoranze, costituzionalismo democratico e democrazia diretta, in ≪GenIUS≫, 2020-1, pp. 1-15. (ISSN 2384-9495)* *11. .Vulnerabilidad personal o contextual? Aproximaciones al analisis de derecho en perspectiva de genero, in ≪Isonomia≫, 51, 2019, pp. 1-28 - (ISSN 1405-0218) – fascia A* ***Book Chapters*** *1. .Entre mas democracia y nueva censura? Primera aproximacion al tema de la cancel culture, in F. Morales, A.Nunez (eds), Libertad de expresion. Un nuevo debate pendiente, Palestra, Lima, 2022, pp. 23-66.* *2. !Porque eres mujer! Trabajo invisible y feminizacion de la pobreza, in C. Fernandez Blanco, E. Pereira Fredes (a cura di) Derecho y pobreza, Marcial Pons, 2021 - ISBN: 9788413812540* *3. Observaciones entorno a la teoria y la practica (del Derecho), in P.A. Ibanez, B. Marciani Burgos, S. Pozzolo, P. Grandez Castro (a cura di), El compromiso constitucional del iusfilosofo: Homenaje a Luis Prieto Sanchis, Palestra, Lima, Peru, 2020, pp. 380-390 (ISBN: 9786123251406).* *4. Avvistamenti dall ' isola che non c ' e, in Mauricio Maldonado, Pau Luque (a cura di), Discutendo con Bruno Celano, vol I, Marcial Pons, Madrid, Spagna, 2020, pp. 337-360 (ISBN 9788491237440).* *5. Neoconstitutionalism, in Encyclopedia of the Philosophy of Law and Social Philosophy, 2019 (ISBN:978- 94-007- 6730-0).* *6. Interpretacion por principios y derechos, in Giovanni Priori Posada (a cura di), Justicia y proceso en el siglo XXI, Palestra editores, Lima, Peru, 2019, pp. 759-774 (ISBN: 9786123250744).*

	7. Prefacion a M. Maldonado Munoz, La democracia a partir de Bobbio, Cevallos Editora Juridica, Quito (Ecuador), 2019 (ISBN: 9789942794130). *8. Interpretazione per principi, tutela dei diritti e ponderazione standard, in A. Saccoccio, S. Cacace (a cura di), Europa e America Latina due continenti, un solo diritto. Unita e specificita del sistema giuridico latinoamericano, Tomo I, Giappichelli, Torino, Tirant Le blach Madrid, 2019 (ISBN/EAN 978-88-921- 3298-6).* *9. Feminismo y disability studies. Una introduccion, in L. Scudieri, L. Guaglianone, R. Escudero, C. Crespo Puras (a cura di), Inclusion socio-laboral de las mujeres con discapacidad, E-Prints Complutense, Junio, 2019, progetto risewise (ISBN 978-84-09-12477-0).* *10. Una riflessione sul costituzionalismo regolativo a partire dall ' America latina in A. Saccoccio, S. Cacace (a cura di), Sistema giuridico latinoamericano. Summer school (Brescia, 9-13 luglio 2018), Giappichelli Torino, 2019, pp. 123-134 (978-8892119949).* *11. Brevi cenni sulla storia della costituzionalizzazione italiana. Conflitti interpretativi e conflitti fra corti, in Luiz Guilherme Marinoni, Ingo Wolfgang Sarlet (a cura di), Processo Constitucional (Portugues), Revista dos Tribunais, Thomson Reuters SauPaulo, Brasil, 2019, § 24, pp. 619-631 (ISBN 9788553213481).* *12. Donne e accesso alla giustizia. Il "vivo" del diritto, in M. Masia, M.V. Sanna (a cura di), Donne e diritto. Un dibattito, AV edizioni, Cagliari, 2019, pp. 371-382 (978-8883741050).* *13. Neokonstytucjonalizm i specyficzność interpretacji konstytucyjnej, in A. Grabowski, J. Holocher (eds.), Studia z teorii konstytucyjnego państwa prawa: konstytucjonalizm, neokonstytucjonalizm, postpozytywizm / Studies from the theory of the constitutional state-of- law: constitutionalism, neoconstitutionalism, postpositivism, Księgarnia Akademicka, Krakow, 2019, pp 83-101 (ISBN 978-83- 7638-988-2).*

Activities in specialist bodies over the last 5 years	*Co-director of the publishing series Postpositivmo y derecho, Palestra Editore, Lima, Peru* *steering committee of the series Refractions. Critical Studies in the History of the Philosophy of Law, ETS, Pisa* *Co-director of the series Law in Question, Ledizioni, Milan*

Name	*Giorgio Pedrazzi*		
Post	*Comparative Private Law Adjunct Professor*		
Academic career	*Research Assistant*	*University of Brescia*	*2004*
	Comparative Private Law Prof.	*University of Brescia*	*2023*
	Law and Data Professor	*University of Brescia*	*2023*
	Private Law Ph.D	*University of Pisa*	*2005*
	Law Degree	*University of Brescia*	*1997*
Employment	*Research assistant*	*University of Brescia*	*2004-present*
Research and development projects over the last 5 years	***Title 2022RPL53N*** *"Demographic and legal changes. Towards an elder law"* *Period 2023-2025* *Partners: University of Insubria (Varese) University of Bari financing 262.484€*		
Industry collaborations over the last 5 years	*N/A*		
Patents and proprietary rights	*N/A*		

Important publications over the last 5 years	https://iris.unibs.it/cris/rp/rp00862 1) *Giorgio Pedrazzi, Clausole tipo per il trasferimento di dati personali verso Paesi terz in M. Confortini, Clausole negoziali, III. Utet Giuridica, 2024 pp. 178-193* 2) *La qualificazione delle criptovalute tra proprietà e circolazione di beni digitali, strumenti finanziari e fiscalità, 2022* 3) *Et al.,Unlock ways to share data on peer review, in Nature, 2020 Feb;578(7796):512-514. doi: 10.1038/d41586-020-00500-y. PMID: 32099126 DOI: 10.1038/d41586-020-00500-y* 4) *Il ruolo del responsabile della protezione dei dati (DPO) nel settore sanitario, in Rivista Italiana di Medicina Legale, 2019, 179* 5) *La cittadinanza digitale: educazione, partecipazione e inclusione, giappichelli, 2019* 6) *Risolvere online le controversie de commercio elettronico, professionalità, 2019*
Activities in specialist bodies over the last 5 years	*University of Brescia* *Data Protection officer* *2019*

Polytechnic University of Milan

Name	*Boris Petrenj*		
Post	*Risk and Resilience Management; Critical Infrastructure Protection; Business Continuity Management;*		
Academic career	*Post-doctoral fellow*	*Politecnico di Milano*	*2014-2019*
	Doctorate (Inter-organisational	*Politecnico di Milano (Italy)*	*2010-2014*

	collaboration for Critical Infrastructure Resilience)		
	MSc in Electrical and Computer Engineering	*University of Novi Sad (Serbia)*	*2009*
Employment	*Senior Researcher*	*Politecnico di Milano, Italy*	*2019-present*
Research and development projects over the last 5 years	***RemLab** – Cooperative Remote Labs Virtual Campus for Higher Education in Engineering, Erasmus+ project, 2022-2024* *KTH Royal Institute of Technology (Sweden), University of Paderborn (Germany)* *90k EUR*		
	***SICt** – Resilience of cross-border Critical Infrastructures, financed by the EC under the Italy-Switzerland Interreg cooperation programme, 2019-2023* *Lombardy Region (Italy), University of Applied Sciences and Arts of Southern Switzerland, Ticino Cantonal police (Switzerland), Canton of Ticino* *2M EUR*		
Industry collaborations over the last 5 years	*European Knowledge Hub and Polity Testbed for Critical Infrastructure Protection (EU-CIP), 2024 - 2025* *Business Continuity Game (validation, promotion and commercialization)*		
	***Supporting Critical Infrastructure Resilience and Disaster-Risk Awareness, Pilot Study on Business Continuity Plans (BCPs),** a consultancy project for the World Bank, funded by Japanese Government through the Global Facility for Disaster Reduction and Recovery (GFDRR), 2019-2021* *NIER Engineering (Italy), Republic of Turkey Ministry of Interior, Disaster and Emergency Management Presidency (AFAD)* *200k EUR*		

Patents and proprietary rights	*Business Continuity Game*	*Simulation-based serious game for training BCM professionals*	*2023*
Important publications over the last 5 years	• ***Petrenj, B.**, Trucco, P. and Feletti, G. (2024) "Enhancing Business Continuity Preparedness Through Experiential Learning: A Serious Game Approach", Proceedings of The Annual European Safety and Reliability conference – ESREL 2024, June 2024, Krakow, Poland* • ***Petrenj, B.**, Piraina, M., Feletti, G. and Trucco, P. (2023) "Information-Sharing in Cross-border Critical Infrastructure Resilience: evaluating the benefits of a digital platform", Proceedings of The Annual European Safety and Reliability conference – ESREL 2023, September 2023, Southampton, UK* • ***Petrenj, B.** and Trucco, P. (2023) "The Potential of Decentralized Autonomous Organizations for Enhancing Inter-organizational Collaborations for Critical Infrastructure Resilience", Proceedings of The Annual European Safety and Reliability conference – ESREL 2023, September 2023, Southampton, UK* • ***Petrenj, B.**, Piraina, M., Borghetti, F., Marchionni, G. & Urbano V. (2023) "Cross-border Digital Platform for Transport Critical Infrastructure Resilience: Functionalities and Use-case", Proceedings of the 20th International Conference on Information Systems for Crisis Response and Management – ISCRAM 2023, May 2023, Omaha (NE), USA.* • *Trucco, P. & **Petrenj, B.** (2023) "Characterisation of Resilience Metrics in full-scale applications to Interdependent Infrastructure Systems", Reliability Engineering and System Safety (RESS), Vol. 235, 109200* • ***Petrenj, B.**, Capone, F., Morsut, C., Di Bucci, D., Polese, M. (2022) "The relevance of Good Practices to improve Disaster Risk Management in Multi-Hazard Risk Scenarios in the field of civil protection", Proceedings of The Annual European Safety and Reliability conference – ESREL 2022, August 2022, Dublin, Ireland.Feletti, G., Piraina, M., **Petrenj, B.** & Trucco, P. (2022) "Collaborative capability building for critical infrastructure resilience: assessment and selection of good practices", Environment Systems and Decisions. https://doi.org/10.1007/s10669-022-09853-3* • *Feletti, G., Piraina, M., **Petrenj, B.** & Trucco, P. (2021) "Good Practices for Critical Infrastructure Resilience: a classification and assessment framework", Proceedings of The Annual*		

	European Safety and Reliability conference – ESREL 2021, September 2021, Angers, France. • ***Petrenj, B.*** *& Trucco, P. (2021) "Blockchain-based Solutions to Support Inter-organisational Critical Infrastructure Resilience", Proceedings of the 18th International Conference on Information Systems for Crisis Response and Management – ISCRAM 2021, May 2021, Blacksburg (VA), USA.* • ***Petrenj, B.****, Piraina, M., Feletti, G., Trucco, P., Urbano V., & Gelmi, S. (2021) "Cross-border Information Sharing for Critical Infrastructure Resilience: Requirements and Platform Architecture", Proceedings of the 18th International Conference on Information Systems for Crisis Response and Management – ISCRAM 2021, May 2021, Blacksburg (VA), USA.* • *Borghetti, F.,* ***Petrenj, B.****, Trucco, P., Calabrese, V., Ponti, M. and Marchionni, G. (2021) "Multi-level approach to assessing the resilience of road network infrastructure" Int. J. Critical Infrastructures, Vol.17, No. 2, pp. 97-132.* • *Fakhruddin, B., Torres, J.,* ***Petrenj, B.****, Tilley, L. (2020) 'Transferability of knowledge and innovation across the world', in: Casajus Valles, A., Marin Ferrer, M., Poljanšek, K., Clark, I. (eds.), Science for Disaster Risk Management 2020: acting today, protecting tomorrow, EUR 30183 EN, Publications Office of the European Union, Luxembourg, 2020* • *Bruinen de Bruin, Y., Vetere Arellano, A.L., Begg, C., Dechy, N., Donovan, A., Kalinowska, K.,* ***Petrenj, B.****, Resch, C., Tulonen, T. (2020) 'Linking actors, sectors and governance levels', in: Casajus Valles, A., Marin Ferrer, M., Poljanšek, K., Clark, I. (eds.), Science for Disaster Risk Management 2020: acting today, protecting tomorrow, EUR 30183 EN, Publications Office of the European Union, Luxembourg, 2020* • *Trucco, P., Maggia, P. and* ***Petrenj, B.*** *(2020) "Adapting public transport to COVID-19 contingencies: evaluating unlock policies in the metropolitan area of Milan through DMCI simulation", Proceedings of The Annual European Safety and Reliability conference (ESREL 2020) and The Probabilistic Safety Assessment and Management conference (PSAM15), June 2020, Venice, Italy.* *https://www.researchgate.net/profile/Boris-Petrenj*		
Activities in specialist bodies over the last 5 years	*Organization for Security and Co-operation in Europe (OSCE)*	*Expert on Counter-Terrorism and P/CVERLT (Rostered)*	*Since 2022*

Name	*Prof. Paolo Trucco*		
Post	*Risk Management*		
Academic career	*Associate Professor* *Assistant Professor* *Doctorate (Quality Engineering)* *Laurea Degree (5 years) in Industrial Engineering*	*Politecnico di Milano* *Politecnico di Milano* *Univ. of Florence* *Politecnico di Milano*	*2005-2014* *2001-2005* *1997-1999* *1994*
Employment	*Full Professor*	*Politecnico di Milano*	*08/2014 – to date*
Research and development projects over the last 5 years	*2024 – reEUman - HORIZON-CL4-2023-TWIN-TRANSITION-01-04, €934,375* *2024 – SpaceItUP - Agenzia Spaziale Italiana-PNRR, €134,666* *2023 - Unlocking the potential of New Space Economy for Circular Economy, National Scientific Research Grants (PRIN) – MUR, €90.174* *2023 - AI4REALNET: AI for REAL-world NETwork operation, HORIZON-CL4-2022-HUMAN-02-01, €456,250* *2022 - ECOSENS - Economic and Societal Considerations for the Future of Nuclear Energy in Society, HORIZON-EURATOM-2021-NRT-01-14, €262,660* *2022 - Capability mapping of the Italian H2 supply chains H2 JRP – Fondazione Politecnico di Milano € 75,000* *2021 - RemLab: Cooperative remote labs virtual campus for higher education in engineering, ERASMUS+ – European Commission, €90,000* *2019 - OHS management systems, workers participation and representativeness under the digital transformation of work, INAIL Research Grant, €734,000*		

	2019 – SmartEU: Operational Model and Tech Platform for the Dynamic Management of Medical Emergency Services, Regione Sicilia – FESR, €3,125,000
Industry collaborations over the last 5 years	*2024 - Space Digital Factory – FaaS Governance Model and market analysis, ThalesAleniaSpace SpA, €150,000* *2024 - LeanEPC - Enhancing critical workflow management through Project Production Management, SAIPEM SpA, €85,000* *2023 - Market and technical analysis of BitApps EO solutions for the Italian market, BitApps (Finland), €48,000* *2023 - Design of a Technology Risk Management Framework for projects, SAIPEM SpA, €75,000* *2022 - Economic assessment modelling of the end-of-life management of rolling stocks., NTV Italo SpA, €100,000* *2022 - Product-Service System design in infrastructure projects driving new space commercialisation, ThalesAleniaSpace SpA, €85.000* *2022 - Unfolding and enacting the value of modularity in satellite space systems, ThalesAleniaSpace SpA, €85.000* *2022 - Assessment of global Supply Chain vulnerability to energy shortage and selection of strategic and tactical measures, Hilti Corporation, €45,000* *2022 - Assessing alternative value chain configurations and business models for EV batteries in Italy, Motus-e, €25,000* *2021 - TechInnoValue 2.0: Extension and refinement of a Methodology for assessing the sustainable value created by the technological innovation in projects SAIPEM SpA, € 80,000* *2020 – TechInnoValue: Methodology for assessing the sustainable value created by the technological innovation in projects, SAIPEM SpA, €100,000* *2020 - Assessment of Emergency Management capabilities and recommendations for improvement , NTV Italo SpA, €150,000* *2019 Development of National Guidelines for Area Business Continuity Plans. Under the programme: Resilience of critical infrastructure and raising awareness on disaster risks, World Bank*

	and Turkish Ministry of Interior Disaster and Emergency Management Authority (AFAD). €200,000		
Patents and proprietary rights	*Business Continuity Game*	*Simulation-based serious game for training BCM professionals*	*2023*
Important publications over the last 5 years	*https://www.scopus.com/authid/detail.uri?authorId=6602279898* *https://scholar.google.it/citations?hl=en&pli=1&user=L0QewzQAAAAJ*		
Activities in specialist bodies over the last 5 years	*ANRA (Italian Association of Risk Managers)* *ANIMP (Italian Association of Industrial Plant Engineering)* *Healthcare Risk Management Committee of the Lombardy Region Government* *Critical Infrastructure Protection and Resilience Technical Committee of the Lombardy Region Government* *Membership without a specific role need not be mentioned*	*Scientific Committee member* *Member of the General Council and of the President's cabinet* *Appointed expert member* *Appointed expert member*	*2024 – date* *2021 – date* *2004 – date* *2011 – date*

Name	Francesca Silvia Carosio		
Post	Teaching area and designation		
Academic career	Lecturer in Health Sociology	Università degli studi di Torino	2019 -2022
	Master II Liv. Big Data & Social Mining	Università di Pisa	2021-2022

	Master's degree in Sociology	Università degli studi di Torino	2018
	Bachelor's degree in history	Università degli studi di Genova	2005
	Master's Degree in arts		2000
Employment	**Project Manager and Researcher**	Cefriel	2022-now
	Project Manager Consultant for management of funded projects	Aosta's Region	2019-2022
		University of Valle d'Aosta	2019-2020
		Freelance	2016-2019
		CSV	2006-2016
Research and development projects over the last 5 years	• 2021, internship at IRPET -CNR (Pisa / Florence): Analysis of territorial dynamics in the pandemic era as an opportunity for peripheral territories through **BigData analysis** (**Facebook Data for Good)**: time clustering, clustering, classification (Python code) • 2020, INAPP, National Institute for the Analysis of Public Policies (Rome): Qualitative assessment of Erasmus applications • 2019, Politecnico di Torino (Turin): Qualitative-quantitative analysis of the "Practices of Ordinary Innovation" of the Politecnico's Architects • 2019 -2020, Fondazione Con il Sud (Rome): evaluation of projects call for volunteers 2019		
Industry collaborations over the last 5 years	• Coordinator and Project Manager Leader at the European level for the HORIZON project M4estro (GA no. 101138506). Industrial Manufacturing As a sErvice STRategies and models for flexible, resilient and reconfigurable value networks through Trusted and Transparent Operations) • Researcher for the European project SEC-AIRSPACE (GA no. 101114635) on the topic of People Analytics as a means of delivering insightful analyses into Human Risk Models within the realm of Cybersecurity for Air Traffic Managers. • Project manager of the project Assolombarda Lavoro 4.0 on topics and training related contents referring to Job 4.0 / 5.0 transizione • Lecturer in data-driven projects and data-driven strategy with GQMA methodology workshop at industrial companies in the province of Trento, FLEXMAN project		
Patents and proprietary rights	• N/A		
Important publications over the last 5 years	• N/A		
	• N/A		

Activities in specialist bodies over the last 5 years	

Name	Frumento Enrico		
Post	Cybersecurity senior researcher and cybersecurity research lead		
Academic career	Lecturer in Founding element of programming	Polytechnic of Milano	1998-2007
	Lecturer on Information security and cyber risk modelling	AIEA/ISACA	2015
	Lecturer in cyber risk modelling and management	CINEAS	2020-2025
	Lecturer at the Information Security Management Master Level II	Cefriel	2015-2020
	Lecturer of Advanced course on Cybersecurity and Cybercrime	Cefriel	2015-present
	Lecturer at the Master of Advanced Studies on Systems, Security and Cybercrime	SUPSI Scuola Universitaria Svizzera Italiana	2020-2022
	Lecturer at the Advanced Studies program on Information Forensics and Modern Cybercrime tactics	SUPSI Scuola Universitaria Svizzera Italiana	2013-present
Employment	Project Manager and Researcher Technical Coordinator	Cefriel	1997-present
	Scientific Coordinator	DOGANA (H2020), Advanced Social Engineering and Vulnerability Assessment	2015-2018

		Framework, as scientific coordinator	
	Technical Coordinator	HERMENEUT (H2020): Enterprises intangible Risks Management via Economic models based on simulation of modern cyber-attacks	2017-2022
	Senior Researcher	CYRUS (GA no. 101100733): Enhancing employees' cybersecurity skills for better protection against cybersecurity attacks	2024-present
	Senior Researcher	Digital4Sustainability (GA no. 101123430)	2024-present
	Senior Researcher	APPTake (DEP 2024): Uptake of Innovative APPlication Security Solutions	2024-present
	Senior Researcher	SEC-AIRSPACE (SESAR JU 2024): Cyber SECurity Risk Assessment in virtualized AIRSPACE scenarios and stakeholders' awareness of building resilient ATM	2024-present
	Senior Researcher	CyberROAD (7th FP) Development of the Cybercrime and Cyberterrorism research roadmap	2013-2015
Research and development projects over the last 5 years	• CyberROAD (7FP- SEC-2013.2.5-1, GA n. 607642) • MUSES (FP7-ICT-2011-8, GA n. 318508) • CYRUS (DIGITAL-2022-TRAINING-02, GA n. 101100733) • SEC-AIRSPACE (HORIZON-SESAR-2022-DES-ER-01-WA1-4, GA n. 101114635) • SEC4AI4SEC (HORIZON-CL3-2022-CS-01-02, GA n. 101120393)		

	• APPTAKE (DIGITAL-ECCC-2022-CYBER-03, GA n. 101128082) • Digital4Sustainability (ERASMUS-EDU-2023-PI-ALL-INNO-BLUEPRINT, GA n. 101140316) • POR Project OK-INSAID, Operational Knowledge from Insights and Analytics on Industrial Data
Industry collaborations over the last 5 years	• Launch of the startup PrOTectME within the framework of EIT-Digital. The company aims to adapt the risk model to protect small and medium enterprises' cyber-physical systems. https://www.protectme-srl.com/ • Development of a QKD rack prototype for Italtel within the framework of EIT-Digital. Q-Secure Net provides quantum secure communication over • metropolitan fiber-optic network with Quantum Key Distribution (QKD). • Researcher for the project OK-INSAID, Operational Knowledge from Insights and Analytics on Industrial Data, funded by the Italian Ministry of Innovation and Research.
Patents and proprietary rights	• N/A
Important publications over the last 5 years	I published 34 papers, cited 169 times, the h-index is 7, and the g-index is 12 (according to Google Scholar). • AA. VV. (2019). "m_Health between reality and future". Springer Innovations in Communication and Computing, P. Perego, G. Andreoni and E. Frumento, Eds., 1st ed. Springer • "The Hidden Cost of Untrusted Vendors in 5G Networks," T. Stuchtey, C. Dörr, E. Frumento, C. Oliveira, G. Panza, S. Rausch, J. Rieckmann and R. Yaich, Brandenburg Institut for Society and Security, Postdam, 2020 • Combatting Cybercrime and Cyberterrorism Challenges, Trends and Priorities AA. VV, Advanced Sciences and Technologies for Security Applications, B. Akhgar and B. Brewster, Eds., 1st ed. Springer, 2016. [Online]. Available: https://www.springer.com/it/book/9783319389295. ISBN 978-3-319-38930-1 • "The Hidden Cost of Untrusted Vendors in 5G Networks," T. Stuchtey, C. Dörr, E. Frumento, C. Oliveira, G. Panza, S. Rausch, J. Rieckmann and R. Yaich, Brandenburg Institut for Society and Security, Postdam, 2020 [Online]. Available: https://www.bigs-potsdam.org/en/research/current-projects/clean-5g/ • The role of SE in the evolution of attacks. Frumento, E., et al. figshare. 2020, Book. https://doi.org/10.6084/m9.figshare.12369248.v1 • "Towards the automation of highly targeted phishing attacks with Adversarial Artificial Intelligence", F. Morano, E. Frumento, DeepSec Conference 2022, 15-18 November 2022, Wien (AT)

	• "Sustainability of cybersecurity for ME&SMEs", E. Frumento, A. Guerini, Proceedings of the GARR Conference 2022, Palermo.		
Activities in specialist bodies over the last 5 years	Researcher an delegate	European CyberSecurity Organisation (ECSO)	2016-2020
	Researcher and Member of the Scientific Committee	European Digital SME Alliance	2020-present
	Member	European Pact for skills Initiative	2023-present

Name	Andrea Guerini		
Post	Cybersecurity Consultant		
Academic career	Certificate of Advanced Studies in Digital Forensics and Cyber Investigation Fundamentals	Berner Fachhochschule	2023
	Master in Strategic Protection of the Country System	Società Italiana per l'Organizzazione Internazionale (SIOI)	2020
	Bachelor in Computer and Network Security	Università degli Studi di Milano	2020
	Master in Global Marketing, Communication & Made in Italy	Centro Studi Comunicare l'Impresa	2017
	Bachelor in Liberal Studies in Communication	Università degli Studi di Milano	2015
Employment	Researcher and Consultant in Cybersecurity	Cefriel	2020 - current
	Researcher and Instructor	CYRUS (GA no. 101100733): Enhancing	2023 - current

		employees' cybersecurity skills for better protection against cybersecurity attacks	
	Researcher and Internal Project Manager	SEC-AIRSPACE (SESAR JU 2024): Cyber SECurity Risk Assessment in virtualized AIRSPACE scenarios and stakeholders' awareness of building resilient ATM	2023 - current
	Researcher	Digital4Sustainability (GA no. 101123430)	2024 - current
	Researcher	Digital4Security	2024 - current
Research and development projects over the last 5 years	- CYRUS (DIGITAL-2022-TRAINING-02, GA n. 101100733) - SEC-AIRSPACE (HORIZON-SESAR-2022-DES-ER-01-WA1-4, GA n. 101114635) - Digital4Sustainability (ERASMUS-EDU-2023-PI-ALL-INNO-BLUEPRINT, GA n. 101140316)		
Industry collaborations over the last 5 years	N/A		
Patents and proprietary rights	N/A		

Important publications over the last 5 years	N/A
Activities in specialist bodies over the last 5 years	N/A

Name	*Domenico Orlando*		
Post	*Cybersecurity & Data Protection Researcher*		
Academic career	*Associate researcher* *ICT law (LLM)* *Master in Law*	*KU Leuven - CITIP* *University of Oslo* *Università Bocconi*	*2019* *2018* *2014*
Employment	*Position* *Cybersecurity researcher* *Digital law consultant* *Associate researcher* *Legal consultant* *In-house lawyer* *Trainee lawyer* *Intern*	*Employer* *CEFRIEL* *Sopra Steria* *KU Leuven – CITIP* *Moores Rowland* *Vivienne Westwood* *Gambino Repetto* *Rossotto Colombatto*	*Period* *2024* *2021-2023* *2019-2021* *2016-2017* *2016* *2014-2016* *2013*
Research and development projects over the last 5 years	*SNIPPET (Secure and Privacy-friendly Peer-to-peer electricity trading)* *2019-2021 https://www.esat.kuleuven.be/cosic/project/snippet/* *Partners: COSIC, ELECTA, IEEL, SMIT, CITIP*		

	ROLECS (Roll Out of Local Energy Communities) *2019-2021 https://leen02.wixsite.com/rolecs* *Partners: ABB, Engie, Farys, KU Leuven, Blixt, Agentschap Innoveren & Onderneren, Innoviris.brussels, VITO, OpenMotics, Metha Advocaten, Anteagroup, Universiteit Gent, EnerGent, Magenta Tree, Ducoop, 70Gigawatt, Ingeium, Fieldfisher, Aspiravi Energy, Powerdale, 3E, Imec, Fluvius, C-valley, Energy Ville, ID Lab, Flux50, KBC, Think-E, Quares, Wattson, VUB, Thermovault*
Industry collaborations over the last 5 years	*Study on Technical Solutions for Organisers of European Citizens Intitiatives* *2023 https://citizens-initiative.europa.eu/sites/default/files/2023-11/Study%20on%20Technical%20Solutions%20for%20Organisers%20of%20European%20Citizens%20Initiatives.pdf* *Partners: Sopra Steria, PWC, DIGIT*
Patents and proprietary rights	*n.a.*
Important publications over the last 5 years	*- Smart meters' roll out, solutions in favour of a trust enhancing law, with W. Vandevelde, March 2021,* DOI:10.19164/jltt.v2i1.1071 *- An Ecosystem View of Peer-to-Peer Electricity Trading: Scenario Building by Business Model Matrix to Identify New Roles, Energies, with Monthakhabi, Zodiri et al., 2021,* https://doi.org/10.3390/en14154438 *- New Roles in Peer-to-Peer Electricity Markets: Value Network Analysis," with Montakhabi et al. in International Energy Conference – ENERGYCon 2020, IEEE, 6 pages, 2020,* DOI:10.1109/ENERGYCon48941.2020.9236480 *The 'by design' turn in EU Cybersecurity Law: emergence, challenges and ways forward, with P. Dewitte, 2019.* ISBN: 9781780688893
Activities in specialist bodies over the last 5 years	*N/A*

Name	*Stefano Rimoldi*		
Post	Cybersecurity Senior Consultant		
Academic career	Master of Science in Management	Bocconi	2016 - 2018
	Bachelor in Economics & Management	Università Cattolica del Scaro Cuore	2011 - 2015
	Business English Higher	Cambridge Assesment Center	2018
Employment	Senior Consultant	Cefriel S.c.a.r.l	October 2023 – Present
	Instructor	Transportation (Incident Management Process training)	October 2023 – present
	Senior Consultant	Energy & Utilities Cyber risk management & Compliance Cyber Maturity Assessment	October 2023 – present
	Senior Consultant	EY S.r.l	2022 – 2023

		Energy & Utilities, Apparel, Consumer Goods Cyber risk management & Compliance Cyber Maturity Assessment IT Risk Audit	
	Consultant	Protiviti S.r.l.	2019 – 2022

	Energy & Utilities, Apparel, Consumer Goods Cyber risk management & Compliance IT Risk Audit
Research and development projects over the last 5 years	None
Industry collaborations over the last 5 years	None
Patents and proprietary rights	None
Important publications over the last 5 years	None

Activities in specialist bodies over the last 5 years	None

University of Koblenz

Name	*Prof. Dr. Jan Jürjens*		
Post	*Professor for Software Engineering*		
Academic career	*Senior Researcher*	*TU München*	*2001*
	PhD (DPhil) (Computer Science)	*Univ. Oxford*	*2004*
	Master (Diplom) (Mathematics with Computer Science)	*Univ. Bremen*	*1998*
Employment	*Professor for Software Engineering*	*Univ. Koblenz*	*2015-*
	Director Research Projects	*Fraunhofer ISST*	*2009-*
	Professor for Software Engineering	*TU Dortmund*	*2009-2015*
	Royal Society Industrial Fellow	*Microsoft Research Cambridge*	*2008-2009*
	non-stipendiary Research Fellow	*Robinson College (University of Cambridge)*	*2008-2009*
	Senior Lecturer	*Open University (UK)*	*2006-2009*
	Senior Researcher	*TU München*	*2001-2006*

Research and development projects over the last 5 years	• *Co-PI: RLP-Forschungskolleg "Data2Health: Trustworthy Data Analytics for Health, 2022-2025 (100.000 EUR).* • *Co-Principal Investigator of Fraunhofer participation: Data Spaces Support Centre (DSSC), DIGITAL-2021-CLOUD-AI-01-SUPPCENTRE, 2022-2026 (1,600,000 EUR).* • *Principal Investigator of Univ. Koblenz participation: RI services to promote deep digitalization of Industrial Biotechnology – towards smart biomanufacturing (BIOINDUSTRY 4.0), HORIZON-INFRA-2022-TECH-01-01, 2023-2027 (247,000 EUR).* • *Principal Investigator of Univ. Koblenz and Fraunhofer ISST participation: DATA Monetization, Interoperability, Trading & Exchange (DATAMITE), HORIZON-CL4-2022-DATA-01-04, 2023-2026* *(1,111,000 EUR).* • *Principal Investigator of Univ. Koblenz participation: Traceability and Explainability of Security in Software Engineering (TraceSEC), DFG, 2023-2026 (304,900 EUR).* • *Principal Investigator of Univ. Koblenz participation: Stakeholders-driven pathways for blockchainimplementation in the agri-food sector (TRUSTyFOOD), HORIZON-CL6-2021-FARM2FORK-01-07, 2022-2025 (142,000 EUR).* • *Principal Investigator of Univ. Koblenz participation: Automated Compliance Checks for Construction, Renovation or Demolition Works (ACCORD), HORIZON-CL4-2021-TWIN-TRANSITION-01-10, 2022-2025 (185,000 EUR).* • *Principal Investigator of Univ. Koblenz participation: Support actions for the set-up of a European data space on skills (DS4Skills), DIGITAL-2021-PREPACTS-DS-01-SKILLS, 2022-2024 (72,000 EUR).* • *Principal Investigator of UKL & ISST participation: Health Data Intelligence: Security and Privacy (AI-NET-PROTECT 4 health), BMBF, 2021-2024 (1,115,000 EUR).* • *Co-Investigator: Engineering and Application of explainable, trustworthy, resilient and secure AI (IH - evrsKI), BMBF, 2021-2025 (200,000 EUR).*

	• *Principal Investigator: Engineering Trustworthy Data-intensive Systems (EnTrust), Forschungsinitiative 2019-2023, RLP, 2019-2023, Univ. Koblenz-Landau, (450,000 EUR).* • *co-Principal Investigator: KI und COVID: Erklärbarkeit und Entscheidungsunterstützung durch KI in Pandemie-Situationen. Ministerium für Wissenschaft, Weiterbildung und Kultur RLP, 2021 - 2023. (180.000 EUR).* • *Principal Investigator of UKL & ISST participation: IIP Ecosphere @ Sec: Sicherheitsaspekte von Plattformen für KI-Ökosysteme in der intelligenten Produktion, BMWi-KI-Wettbewerb, 2020-2023 (479.000 EUR).* • *Principal Investigator of UKL & ISST participation: A Data Platform for the Cognitive Ports of the Future (DataPorts), EU-Horizon-2020, 2020-2022 (592,818 EUR).* • *Principal Investigator of UKL & ISST participation: Trusted Secure Data Sharing Space (TRUSTS),EU-Horizon-2020, 2020-2022 (173,250 EUR).* • *Principal Investigator of ISST participation: Ein KI-basiertes Serviceökosystem für technischen Service im Zeitalter von Industrie 4.0 (ServiceMeister), BMWi-KI-Wettbewerb, 2020-2022 (105,000 EUR).* • *Principal Investigator of UKL & ISST participation: EXplainable AI for automated Production Systems (XAPS), BMBF, 2020-2022 (305.000 EUR).* • *Principal Investigator of UKL & ISST participation: Digital Reality in Zero Defect Manufacturing (QU4LITY), EU-Horizon-2020, 2019-2022 (269,150 EUR).* • *Principal Investigator of ISST participation & Member of Steering Board: Industrie 4.0 Recht-Testbed: Juristische Testumgebung und offenes Repository (I40RTB), BMWi, 2019-2022 (960,000 EUR).* • *Principal Investigator of ISST participation: A European AI On Demand Platform and Ecosystem (AI4EU), EU-Horizon-2020, 2019-2022.* • *Principal Investigator: European Railway Data Space, voestalpine SIGNALING Siershahn GmbH, Universität Koblenz-Landau, 2017–2022 (ca. 150.000 EUR).*

	• *Principal Investigator of ISST participation: AdditiveManufacturABLE (aMable), EU-Horizon-2020: Factories of the Future, 2017-2022 (130,000 EUR).* *Principal Investigator: Datenschutz-konforme Indoor-Lokalisierung und Tracking von Personen (DILoTra), InnoProm, RLP/EFRE, 2019-2022 (200,000 EUR), Univ. Koblenz-Landau.* • *Principal Investigator: T-REQS: Template-based REquirements Quality improvement in Space engineering supported by an ontology-based requirements meta-model, Networking/Partnering* *Initiative of the European Space Agency (ESA), Universität Koblenz-Landau, 2016–2022 (ca. 90.000 EUR).* • *Member of Project Management Board: Industrial Data Space Plus: Architekturtopologien für Datensouveränität in Geschäftsökosystemen auf Basis des Industrial Data Space (InDaSpace-Plus). Funded by the German Ministry of Education and Research (BMBF): 4,943,861 EUR, 2017-2020 (Fraunhofer ISST).* • *Principal Investigator of UKL participation: Beyond One-Shot Security: Requirements-driven Run-time Security Adaptation to Reduce Code Patching (SecVolution @ Run-Time), DFG Priority Program 1593 "Design for Future – Managed Software Evolution", Universität Koblenz-Landau, 2016–2020 (292,700 EUR).*
Important publications over the last 5 years	https://dblp.org/pid/j/JanJurjens.html https://scholar.google.com/citations?user=erI33mgAAAAJ&hl=en&oi=ao *[B05] M. Salnitri, J. Jürjens, H. Mouratidis, L. Mancini, P. Giorgini. Visual Privacy Management: Design and Applications of a Privacy-Enabling Platform. Lecture Notes in Computer Science, Security and Cryptology sub series (LNCS, volume 12030), 2020, 149 pp.* *[J44] S. Peldszus, J. Bürger, J. Jürjens. UMLsecRT: Reactive Security Monitoring of Java Applications With Round-Trip Engineering. In IEEE Trans. Software Eng.. vol. 50 no. 1: pp. 16–47 (2024)* *[J43] Q. Ramadan, M. Konersmann, A. S. Ahmadian, J. Jürjens, S. Staab. MBFair: A model-based verification methodology for detecting violations of individual fairness. In Software and Systems Modeling (Springer). 2024.*

	[J42] K. Großer, A. S. Ahmadian, Q. Ramadan, J. Jürjens. Benchmarking Requirement Template Systems: Comparing Appropriateness, Usability, and Expressiveness. In Requirements Engineering Journal, 2024. *[J41] A. von Gladiss, A. S. Ahmadian, J. Jürjens. Image reconstruction in a data space for MPI. In International Journal on Magnetic Particle Imaging IJMPI, Vol. 10 No. 1 Suppl. 1 (2024). Abstract.* *[J40] Z. Boukhers, P. Goswami, J. Jürjens. Knowledge Guided Multi-filter Residual Convolutional Neural Network for ICD Coding from Clinical Text. In Neural Computing and Applications, Springer. 2023.* *[J39] H. Hasso, K. Großer, I. Aymaz, H. Geppert, J. Jürjens. Enhanced Abbreviation-Expansion Pair Detection for Glossary Term Extraction. In Information and Software Technology, 2023.* *[J38] J. Stocker, N. Herda, J. Jürjens. Lifecycle and metrics to measure the resilience of business processes by considering resources. In Business Process Management Journal, 2022.* *[J37] Z. Boukhers, T. Hartmann, J. Jürjens. COIN: Counterfactual Image Generation for Visual Question Answering Interpretation. In Sensors. 2022.* *[J36] K. Tuma, S. Peldszus, R. Scandariato, D. Strüber, J. Jürjens. Checking Security Compliance between Models and Code. In Software and Systems Modeling (Springer).* *[J35] K. Großer, V. Riediger, J. Jürjens. Requirements Document Relations: A Reuse Perspective on Traceability through Standards. In Software and Systems Modeling (Springer). 2022. Accepted for presentation at the RE 2022 journal-first track.* *[J34] S. Peldszus, J. Bürger, T. Kehrer, J. Jürjens. Ontology-Driven Evolution of Software Security. In Data & Knowledge Engineering (Elsevier). Special issue on selected publications at RCIS'2020, vol. 134, July 2021.* *[J33] M.S. Sadi, W. Ahmed, J. Jürjens. Towards Tolerating Soft Errors for Embedded Systems. In Springer Nature Computer Science, vol. 2 no. 1, 2021.*

	[J32] S. Pape, F. Paci, J. Jürjens, F. Massacci. Selecting a Secure Cloud Provider – An Empirical Study and Multi Criteria Approach. In Information. Special Issue "Cloud Security Risk Management", 2020, 28 pp.. *[J31] Q. Ramadan, D. Strüber, M. Salnitri, J. Jürjens, V. Riediger, S. Staab. A Semi-Automated BPMN-based Framework for Detecting Conflicts between Security, Data-Minimization and Fairness Requirements. In Journal of Software and Systems Modeling (SoSyM) (Springer Verlag). Invited for journal special issue with best papers of ECMFA'17 and ECMFA'18, 2020, 35 pp.* *[C130] M. Lohr, S. Peldszus, J. Jürjens, S. Staab. 'Fast, Favorable, and Fair Blockchain-based Exchange of Digital Goods using State Channels. In IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2024), IEEE, 2024.* *[C129] M. R. Sama, E. Lyczkowski, M. Petry, W. Kiess, J. Jürjens. 5G-enabled Flexible Security Framework for Industrial Applications. In International Conference on Communications (ICC), IEEE, 2024.* *[C128] A. S. Ahmadian, S. Franke, C. N. Gnoguem, J. Jürjens. Privacy-Friendly Sharing of Health Data Using a Reference Architecture for Health Data Spaces. In Eclipse Security, AI, Architecture and Modelling 2024 on Dataspaces, 2024.* *[C127] K. Großer, M. Rukavitsyna, J. Jürjens. A Comparative Evaluation of Requirements Template Systems. In IEEE International Requirements Engineering Conference (RE), IEEE, 2023.* *[C126] Z. Boukhers, A. Bouabdallah, C. Yang, J. Jürjens. Beyond Trading Data: The Hidden Influence of Public Awareness and Interest on Cryptocurrency Volatility. In 32nd ACM International Conference on Information and Knowledge Management (CIKM '23), ACM, 2023.* *[C125] K. Vernickel, M. Singh, M. Konersmann, J. Jürjens. Ontology-Based Synchronization Of Automated Production Systems And Their Simulation Model. In IEEE International Requirements Engineering Conference (RE), 2023.* *[C124] M.R. Sama, W. Kiess, R. Guerzoni, S. Thakolsri, J. Jürjens. Redefining the Trust Model for the Internet of Everything in the 6G*

	era. In IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, 2022. *[C123] M. Lohr, K. Skiba, M. Konersmann, J. Jürjens, S. Staab. Formalizing Cost Fairness for Two-Party Exchange Protocols using Game Theory and Applications to Blockchain. In IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2022), IEEE, 2022.* *[C122] M. Konersmann, A. Kaplan. T. Kühn, R. Heinrich, A. Koziolek, R. Reussner, J. Jürjens, M. al-Doori, N. Boltz, M. Ehl, D. Fuchß, K. Großer, S. Hahner, J. Keim, M. Lohr, T. Saglam, S. Schulz, J.-P. Töberg. Evaluation Methods and Replicability of Software Architecture Research Objects. In 19th IEEE International Conference on Software Architecture (ICSA 2022), IEEE, 2022.* *[C121] H. Hasso, K. Großer, I. Aymaz, H. Geppert, J. Jürjens. Abbreviation-Expansion Pair Detection for Glossary Term Extraction. In 28th International Working Conference on Requirement Engineering: Foundation for Software Quality (REFSQ 2022), Springer, LNCS, 2022. Invited for submission as a revised and extended version to the special section on REFSQ 2022 best papers of Elsevier's Information and Software Technology Journal (IST).* *[C120] M.R. Sama, R. Guerzoni, W. Kiess, S. Thakolsri, J. Jürjens. Why is Application Reliability an Issue for an Ultra-Reliable 6G Network ? In 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), IEEE, 2021.* *[C119] M. Lohr, B. Schlosser, J. Jürjens, S. Staab. Cost Fairness for Blockchain-Based Two-Party Exchange Protocols. In IEEE Blockchain 2020, IEEE, 2020.* *[C118] J. Bürger, T. Kehrer, J. Jürjens. Ontology Evolution in the Context of Model-based Secure Software Engineering. In 14th International Conference on Research Challenges in Information Science (RCIS 2020), Springer LNBIP, 2020, 16 pp.. [Acceptance rate 19/118=16%. Nominated for distinguished paper award and invited for special journal issue.]* *[C117] S. Peldszus, K. Tuma, D. Strüber, J. Jürjens, R. Scandariato. Secure Data-Flow Compliance Checks between Models and Code based on Automated Mappings. In ACM/IEEE 22th International*

	Conference on Model Driven Engineering Languages and Systems (Models 2019), ACM, 2019, 10 pp.. [Acceptance rate 19%.] *[C116] M. Lohr, J. Hund, J. Jürjens, S. Staab. Ensuring Genuineness for Selectively Disclosed Confidential Data using Distributed Ledgers: Applications to Rail Wayside Monitoring. In IEEE Blockchain 2019, IEEE, 2019.* *[C115] S. Ahmadian, D. Strüber, J. Jürjens. Privacy-Enhanced System Design Modeling Based on* *Privacy Features. In 34th ACM/SIGAPP Symposium On Applied Computing (ACM SAC 2019), ACM, 2019.* *[C114] R. Afrin, M.S. Sadi, J. Jürjens. An Efficient Soft Error Tolerant Approach to Enhance Reliability of TCAM. In: 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT-2019), IEEE, 2019.*

Mykolas Romeris University

Name	*Marius Laurinaitis*		
Post	*Teaching area and designation* *Professor Mykolas Romeris University, Vilnius (Lithuania)* *MRU LegalTech Center*		
Academic career	*31/08/1999 – 31/05/2003* *31/08/2003 – 31/01/2005* *30/09/2010 – 30/09/2014*	*Bachelor of Law Mykolas Romeris University* *Master of Law Mykolas Romeris University* *Doctor of Social Science, IT Law, PhD Mykolas Romeris University*	
Employment	*Position* *Professor*	*Employer* *Mykolas Romeris University, Vilnius (Lithuania)*	*Period* *31/01/2005 – CURRENT*
Research and development projects over the last 5 years	■ *January 15, 2024 - September 30, 2026, Senior Research Fellow for the project "Developing and deploying SOC capabilities for the academic sector - a teamwork of Universities and RTOs in the CEE region (SOCCER)".* ■ *October 2023 - September 2027, Senior Research Fellow / project manager for the project "DIGITAL4Security – European Masters Programme in Cybersecurity Management & Data Sovereignty"* ■ *April 2023 to October 2025, Senior Research Fellow / project manager for the project Project DI4 LITHUANIAN ID "Digital Innovation for Lithuanian Industrial Development (DI4 LITHUANIAN ID)"* ■ *DVITAS (Bilingual Automatic Terminology Extraction) is a project implemented by the researchers of Vytautas Magnus*		

	University and Mykolas Romeris University and funded by the Research Council of Lithuania. 2020 - 2022. ■ *2021–2023 The State Data Protection Inspectorate, together with Mykolas Romeris University, is implementing the SolPriPa 2 WORK project "Addressing the Privacy Paradox 2: Promoting High Standards of Data Protection as a Fundamental Right in the Workplace". 2021 - 2023.*
Important publications over the last 5 years	*Please link your research gate profile or any other official website that lists your publications.* • *Laurinaitis, Marius; Štitilis, Darius; Warren, Matt; Khan, Shah Khalid. Hybrid Threats — The New Generation of Threats // International Journal of Contemporary Intelligence Issues : Australian Institute of Professional Intelligence Officers. ISSN 2981-9717. 2024, vol. 1, no. 2, p. 56-68.* • *Štitilis, Darius; Laurinaitis, Marius; Malinauskaitė-van de Castel, Inga; Warren, Matthew. Navigating the Cyber Front: Belarus' State Control and Emerging Cyber Threats // Proceedings of the 23rd European Conference on Cyber Warfare and Security, ECCWS 2024 : Academic Conferences International Limited. ISSN 2048-8602. eISSN 2048- 8610. 2024, vol. 23, no. 1, p. 542-551. DOI: 10.34190/eccws.23.1.2518.* • *Štitilis, Darius; Laurinaitis, Marius; Warren, Matthew. Hybrid Cyber Threats: Lithuanian Context // Journal of information warfare. Virginia : ArmisteadTEC. ISSN 1445-3312. eISSN 1445-3347. 2024, vol. 23, iss. 1, Journal of Information Warfare (2024) 23.1: 77-94, p. 77-94. Prieiga per internetą: <https://www.jinfowar.com/journal/volume-23-issue-1/hybrid-cyber-threats-lithuanian-context>.* • *Štitilis, Darius; Laurinaitis, Marius; Verenius, Egidijus. The use of biometric technologies in ensuring the security of critical Infrastructure: the context of the protection of personal data // Entrepreneurship and sustainability issues : Entrepreneurship and Sustainability Center. eISSN 2345-0282. 2023, vol. 10, iss. 3, p. 133-150. DOI: 10.9770/jesi.2023.10.3(10).* • *Warren, Matt; Štitilis, Darius; Laurinaitis, Marius. The Impact of Russian Cyber Attackers within the Ukraine Situation // Journal of information warfare. Virginia : ArmisteadTEC. ISSN 1445-3312. eISSN 1445-3347. 2023, vol. 22, iss. 1, p. 88-106. Prieiga per internetą:*

	<https://www.jinfowar.com/journal/volume-22-issue-1/impact-russiancyber-attackers-within-ukraine-situation>

International University of La Rioja

Name	*Prof. Dr. Facundo Gallo Serpillo*		
Post	*Teaching area and designation*		
Academic career	*Doctorate (PhD in criminology)*	*Universidad de Granada*	*2024*
	Master degree (MSc in cybersecurity)	*Universidad Internacional de Valencia*	*2019*
	Master degree (MSc in scientific dissemination)	*Universitat Oberta de Catalunya*	*2017*
	Undergraduate degree (BSc in Information Technologies)	*University of Wales*	*2015*
Employment	*Full professor*	*Universidad Internacional de la Rioja*	*2024 -*
	Part-time professor	*Universidad Miguel Hernández*	*2024 -*
	Co-founder|CSO	*Ewala IT Services*	*2021 -*
Research and development projects over the last 5 years	*Digital4Security– European Masters Programme in Cybersecurity, Management & Data Sovereignty, DIGITAL-2022-SKILLS-03, 2023 - 2026.* *Ingenious- Horizon 2020- Part of GRANT_NUMBER: 833435 | https://ingenious-first-responders.eu/. 2024* *NEOTEC – Centro para el Desarrollo Tecnológico y la Innovación – 2023-2024* *Mine.the.Gap – Horizon 2020- Part of GRANT_NUMBER: 873149 | https://h2020-minethegap.eu/wp-content/uploads/2020/12/Factsheet_MinesKeeper.pdf. 2022-2023* *EBT- Centro Europeo de Empresas e Innovación del Principado de Asturias – 2021-2023*		

Industry collaborations over the last 5 years	*Project title* *Partners*
Patents and proprietary rights	*Title KARONT3 DATA LEAK OBSERVATORY* *Year 2024*
Important publications over the last 5 years	*Facundo Gallo-Serpillo. 2024. Estudio demográfico del child grooming en España mediante interacción encubierta en Chats. Anuario de Justicia de Menores. Astigi. 2023.* *Facundo Gallo-Serpillo; Javier Valls-Prieto. 2024. Analysis of CSEM offenders on the dark web using honeypots to geolocate IP addresses from Spain. Computers in Human Behavior. ELSEVIER. 154, pp.1-10.* *Javier Valls-Prieto; Facundo Gallo-Serpillo. 2022. El arte de pescar en aguas profundas: Metodología de investigación criminológica basada en Dark Web y Honeypots. Cuadernos de Política Criminal. Dykinson. 138, pp.223-253.* *Facundo Gallo. 2020. Deep Web. El monstruo de la red. Editorial Ra-Ma. Ra-Ma*
Activities in specialist bodies over the last 5 years	*Organisation: ISACA* *Role* *Period: 2020-*

Name	*Fidel Paniagua Diez*		
Post	*Software Engineering and Cybersecurity Area* *Director of MSc in Cybersecurity*		
Academic career	*Doctorate*	*Universidad Carlos III de Madrid*	*2020*
	Master degree (MSc in telematic engineering)	*Universidad Carlos III de Madrid*	*2014*
	Undergraduate degree (BSc in Computer Science)		*2011*

		Universidad Carlos III de Madrid	
Employment	*Head of Cybersecurity* *Professor and Director of MSc in Cybersecurity* *Researcher*	*Clover Technologies* *UNIR* *UC3M*	*2016 - current* *2015 – current* *2010 - 2020*
Research and development projects over the last 5 years	*Researcher* *2024 - current*	*Digital4Security*	
Industry collaborations over the last 5 years	*N/A*		
Patents and proprietary rights	*Blockchain-based system for issuing and validating certificates*		*2019*
Important publications over the last 5 years	*Diez, F. P. (2020). Advanced AAA System for interoperable distributed architectures (Doctoral dissertation, Universidad Carlos III de Madrid).* *González Domínguez, P., Paniagua Diez, F., Suarez Touceda, D., & Nombela Pérez, J. J. (2020) Development of a Methodology to Securitize Smart Toys in Household Environments, CIBSI-TIBETS-20, Bogota* *Paniagua Diez, F., Viedma Astudillo, M. (May 2019). A blockchain-based platform for the secure coordination of a robotic swarm, Digital Enterprise Show, Madrid.* *Paniagua Diez, F., Suarez Touceda, D., Sierra Camara, J. M., & Zeadally, S. (January 2019). Lightweight Access Control System for Wearable Devices, IT Professional, 21(1), 50-58.*		
Activities in specialist bodies over the last 5 years	*N/A*		

Name	*Javier Bermejo Higuera*		
Post	*Cybersecurity*		
Academic career	*Electronic Engineer's Degree* Habilitation *[German post-doctoral qualification] (subject)*	*Alcala University*	*2000*
		Institution	*Year*
		Institution	*Year*
	Doctorate (PhD) armament	*Polytechnic School of the Army*	*2016*
	Undergraduate degree (subject)		
Employment	*Full Professor*	*UNIR*	*2024*
Research and development projects over the last 5 years	*- Software architecture for optimised and secure data analysis using Cloud and Edge infrastructures (Cloud2Edge). Call for UNIR Research RETOS Projects 2019.* *- Secure Exploitation of Open Data from Smart Devices in the Future Internet Society (SecOpenData). Call for UNIR Research Challenges Projects 2021.* *- European Global Interference Protection Network (EGIPRON). EUROPEAN COMMISSION EUROPE HORIZON PROJECT 2021.* *- Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation (STRIKE3). EUROPEAN COMMISSION H2020 PROJECT 2016*		
Industry collaborations over the last 5 years	*Project title* *Partners*		
Patents and proprietary rights	*Title*		*Year*
Important publications over the last 5 years	• *Ortiz-Ruiz, E., Bermejo, J. R., Sicilia, J. A., & Bermejo, J. (2024). Machine Learning Techniques for Cyberattack Prevention in IoT Systems: A Comparative Perspective of Cybersecurity and Cyberdefense in Colombia. Electronics, 13(5), 824.*		

	• *González Arias, Rafael, et al. "Systematic Review: Anti-Forensic Computer Techniques." Applied Sciences 14.12 (2024): 5302.* • *Bermejo Higuera, J., Morales Moreno, J., Bermejo Higuera, J. R., Sicilia Montalvo, J. A., Barreiro Martillo, G. J., & Sureda Riera, T. M. (2024). Benchmarking Android Malware Analysis Tools. Electronics, 13(11), 2103.* • *Maestre, R. J., Bermejo Higuera, J., Gámez Gómez, N., Bermejo Higuera, J. R., Sicilia Montalvo, J. A., & Orcos Palma, L. (2023). The application of blockchain algorithms to the management of education certificates. Evolutionary Intelligence, 16(6), 1967-1984.* • *Masid, A. G., Higuera, J. B., Higuera, J. R. B., & Montalvo, J. A. S. (2023). Application of the SAMA methodology to Ryuk malware. Journal of Computer Virology and Hacking Techniques, 19(2), 165-198. Masid, A. G., Higuera, J. B., Higuera, J. R. B., & Montalvo, J. A. S. (2023). Application of the SAMA methodology to Ryuk malware. Journal of Computer Virology and Hacking Techniques, 19(2), 165-198.* • *Moya, C. V., Bermejo Higuera, J. R., Bermejo Higuera, J., & Sicilia Montalvo, J. A. (2023). Implementation and Security Test of Zero-Knowledge Protocols on SSI Blockchain. Applied Sciences, 13(9), 5552.* • *Riera, T. S., Higuera, J. R. B., Higuera, J. B., Herraiz, J. J. M., & Montalvo, J. A. S. (2022). A new multi-label dataset for Web attacks CAPEC classification using machine learning techniques. Computers & Security, 120, 102788.* • *Sureda Riera, T., Bermejo Higuera, J. R., Bermejo Higuera, J., Sicilia Montalvo, J. A., & Martínez Herráiz, J. J. (2022). Systematic Approach for Web Protection Runtime Tools' Effectiveness Analysis. CMES-Computer Modeling in Engineering & Sciences, 133(3).* • *Higuera, J. R. B., Higuera, J. B., García, J. L. T., Montalvo, J. A. S., & Rubio, M. S. (2022). Building a dataset through attack pattern modeling and analysis system. Computers & Electrical Engineering, 97, 107614.* • *Rodríguez, M. Á. S., Higuera, J. B., Higuera, J. R. B., Montalvo, J. A. S., & Crespo, R. G. (2021). A systematic approach to analysis for assessing the security level of cyber-physical systems in the electricity sector. Microprocessors and Microsystems, 87, 104352.* • *Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S., Riera, T. S., Argyros, C. I., & Magrenán, A. A. (2021). Combinatorial Method with Static Analysis for Source Code Security in Web*

	Applications. CMES-Computer Modeling in Engineering & Sciences, 129(2), 541-565. • *Motero, C. D., Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S., & Gómez, N. G. (2021). On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey. IEEE Access, 9, 109289-109319.* • *de Vicente Mohino, J. J., Bermejo-Higuera, J., Bermejo Higuera, J. R., Sicilia, J. A., Sánchez Rubio, M., & Martínez Herraiz, J. J. (2021). Mmale—a methodology for malware analysis in linux environments. Computers, Materials & Continua, 67(2), 1447-1469.* • *Ibarra-Fiallos, S., Higuera, J. B., Intriago-Pazmiño, M., Higuera, J. R. B., Montalvo, J. A. S., & Cubo, J. (2021). Effective filter for common injection attacks in online web applications. IEEE Access, 9, 10378-10391.* • *Piedrahita-Valdés, H., Piedrahita-Castillo, D., Bermejo-Higuera, J., Guillem-Saiz, P., Bermejo-Higuera, J. R., Guillem-Saiz, J., ... & Machío-Regidor, F. (2021). Vaccine hesitancy on social media: Sentiment analysis from June 2011 to April 2019. Vaccines, 9(1), 28.* • *Montes, F., Bermejo, J., Sanchez, L. E., Bermejo, J. R., & Sicilia, J. A. (2021). Detecting Malware in Cyberphysical Systems Using Machine Learning: a Survey. KSII Transactions on Internet and Information Systems (TIIS), 15(3), 1119-1139.* • *Mateo Tudela, F., Bermejo Higuera, J. R., Bermejo Higuera, J., Sicilia Montalvo, J. A., & Argyros, M. I. (2020). On combining static, dynamic and interactive analysis security testing tools to improve OWASP top ten security vulnerability detection in web applications. Applied Sciences, 10(24), 9119.* • *Piedrahita Castillo, D., Regidor, F. M., Higuera, J. B., Higuera, J. R. B., & Montalvo, J. A. S. (2020). A new mail system for secure data transmission in cyber physical systems. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 28(Supp02), 23-48.* • *Correa, R., Bermejo Higuera, J. R., Higuera, J. B., Sicilia Montalvo, J. A., Rubio, M. S., & Magreñán, Á. A. (2021). Hybrid security assessment methodology for web applications. Computer Modeling in Engineering & Sciences, 126(1), 89-124.* • *Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S., Villalba, J. C., & Pérez, J. J. N. (2020). Benchmarking Approach to Compare Web Applications Static Analysis Tools Detecting OWASP Top Ten Security Vulnerabilities. Computers, Materials & Continua, 64(3).*

	• *Sureda Riera, T., Bermejo Higuera, J. R., Bermejo Higuera, J., Martínez Herraiz, J. J., & Sicilia Montalvo, J. A. (2020). Prevention and fighting against web attacks through anomaly detection technology. A systematic review. Sustainability, 12(12), 4945.* • *Bermejo Higuera, J., Abad Aramburu, C., Bermejo Higuera, J. R., Sicilia Urban, M. A., & Sicilia Montalvo, J. A. (2020). Systematic approach to malware analysis (SAMA). Applied Sciences, 10(4), 1360.* • *de Vicente Mohino, J., Bermejo Higuera, J., Bermejo Higuera, J. R., & Sicilia Montalvo, J. A. (2019). The application of a new secure software development life cycle (S-SDLC) with agile methodologies. Electronics, 8(11), 1218.*
Activities in specialist bodies over the last 5 years	*Organisation Role Period* *Membership without a specific role need not be mentioned*

Name	*Sergio Mauricio Martinez Monterrubio*		
Post	*Cybersecurity*		
Academic career	*Computer science*	*UNAM, Mexico*	*1998*
	MBA	*Newport University, USA*	*2002*
	Doctorate (PhD) Computer Science	*ITESM, Mexico*	*2016*
	PostDoctorate	*UCM, Madrid Spain*	*2017-2020*
Employment	*Full Professor*	*UNIR*	*2020*
Research and development projects over the last 5 years	*DIGITAL4SECURITY H2027* *Universidad Internacional de La Rioja* *since 04/09/2023*		

	PERXAI: PERSONALIZACION DE INTELIGENCIA ARTIFICIAL EXPLICABLE MEDIANTE CONOCIMIENTO EXPERIMENTAL - PID2020-114596RB-C21 *Agencia Estatal de Investigación* *01/11/2021* *EXPLAINABLE CBR* *Universidad Complutense de Madrid* *01/09/2018* *RAMSES un proyecto H2020* *Universidad Complutense de Madrid* *01/11/2017*
Industry collaborations over the last 5 years	
Patents and proprietary rights	
Important publications over the last 5 years	*STEG-XAI: explainable steganalysis in images using neural networks* *Multimedia Tools and Applications* *2023-11-07 | Journal article* *DOI: 10.1007/s11042-023-17483-3* *CONTRIBUTORS: Eugenia Kuchumova; Sergio Mauricio Martínez-Monterrubio; Juan A. Recio-Garcia* *Systematic review of SIEM technology: SIEM-SC birth* *International Journal of Information Security* *2023-01-02 | Journal article*

	DOI: 10.1007/s10207-022-00657-9 *Part of ISSN: 1615-5262* *Part of ISSN: 1615-5270* *CONTRIBUTORS: Juan Miguel López Velásquez; Sergio Mauricio Martínez Monterrubio; Luis Enrique Sánchez Crespo; David Garcia Rosado* *Coronavirus fake news detection via MedOSINT check in Health care official Bulletins with CBR explanation* *Information Sciences* *2021-06-17 | Journal article* *DOI: 10.1016/j.ins.2021.05.074* *Part of ISSN: 0020-0255* *Methodology for Computer Security Incident Response Teams into IoT Strategy* *KSII Transactions on Internet and Information Systems* *2021-05-31 | Journal article* *DOI: 10.3837/tiis.2021.05.018* *Part of ISSN: 1976-7277* *Black Widow Crawler for TOR network to search for criminal patterns* *2021 Second International Conference on Information Systems and Software Technologies (ICI2ST)* *2021-03-17 | Journal article* *DOI: 10.1109/ici2st51859.2021.00023* *ISBN: 9781665404112*

	Handbook of Research on Machine and Deep Learning Applications for Cyber Security *Advances in Information Security, Privacy, and Ethics* *2020 | Book chapter* *DOI: 10.4018/978-1-5225-9611-0* *Part of ISBN: 9781522596110* *Part of ISBN: 9781522596134* *Part of ISSN: 1948-9730* *Part of ISSN: 1948-9749* *Anomaly-Based Intrusion Detection* *2020 | Book chapter* *DOI: 10.4018/978-1-5225-9611-0.ch010* *CONTRIBUTORS: Jorge Maestre Vidal; Marco Antonio Sotelo Monge; Sergio Mauricio Martínez Monterrubio* *EsPADA: Enhanced Payload Analyzer for malware Detection robust against Adversarial threats* *Future Generation Computer Systems* *2020-03 | Journal article* *DOI: 10.1016/j.future.2019.10.022* *Part of ISSN: 0167-739X* *Explainable Prediction of Chronic Renal Disease in the Colombian Population Using Neural Networks and Case-Based Reasoning* *IEEE Access* *2019 | Journal article*

	DOI: 10.1109/access.2019.2948430 *Part of ISSN: 2169-3536* *Profits at the Dawn of Cybercrime-as-a-Service* *2019 International Conference on Information Systems and Software Technologies (ICI2ST)* *2019-11 | Journal article* *DOI: 10.1109/ici2st.2019.00017* *ISBN: 9781728148861* *MRlog Method for Computer Security for Electronic Medical Records with Logic and Data Mining* *BioMed Research International* *2015 | Journal article* *DOI: 10.1155/2015/542016* *CONTRIBUTORS: Sergio Mauricio Martínez Monterrubio; Juan Frausto Solis; Raúl Monroy Borja*
Activities in specialist bodies over the last 5 years	*Organisation* *Role* *Period* *UNIR* *SEC cybersecurity group Director* *2024 - present*

Brno University of Technology

Name	*František Kasl*		
Post	*Post-doc Researcher and Lecturer*		
Academic career	***Ph.D.*** *- (Law of information and communication technologies, intern Ph.D. studies, dissertation topic: "Legal and Economic Aspects of Personal Data Breach in the Context of the Internet of Things")*	*Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic*	*2021*
	JUDr. *- (Law of Information and Communication technologies)*	*Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic*	*2021*
	Ing. *– (International Business and Enterprise Valuation)*	*Faculty of International Relations, University of Economics, Prague, Czech Republic*	*2014*
Employment	*Researcher*	*Centre for Education, Research and Innovation in Information and Communication Technologies-ExecUnit, Faculty of Informatics, Masarykova univerzita, Žerotínovo náměstí 9, 601 77 Brno, Czech Republic*	*2017 – present*
	Lecturer		*2021 - present*
	Researcher and Lecturer	*Faculty of Electrical Engineering and Communication Technologies, Brno University of Technology, Technická 3058/10, 616 00 Brno, Czech Republic*	*2017 - present*
		Institute of Law and Technology, Faculty of Law, Masaryk	

	University, Brno, Czech Republic
Research and development projects over the last 5 years	*Selected projects:* *RES-Q Registry for Stroke Care Quality upgrade for stroke care improvement (101057603)* *Capacity building in cybersecurity (VJ03030052)* *Data Flow Protection in Shared Transport Vehicles (CK03000040)* *Sector Skills Alliances 2020 (621701-EPP-1-2020-1-LT-EPPKA2-SSA-B)* *Load management in a distributed energy environment (TK04020195)* *Secure power flexibility for grid control and market purposes (TK01030078)* *National Qualification Framework in Cybersecurity (VI20192022161)* *Legal and Technical Means to Protect Privacy in Cyberspace (TL02000398)* *INFORM - European Academy of ICT law (763866)* *Full list of projects including description available here:* *https://www.muni.cz/en/people/462266-frantisek-kasl/projects*
Industry collaborations over the last 5 years	*Selected projects:* *DP16_Cybersecurity Vulnerability Disclosure and Related Procedures (Bugbounty) (MUNI/33/DP16/2021)* *DP10_Compliance Programme for SMEs (MUNI/33/DP10/2020)* *Load management in a distributed energy environment (TK04020195)* *Secure power flexibility for grid control and market purposes (TK01030078)* *Full list of projects including description available here:* *https://www.muni.cz/en/people/462266-frantisek-kasl/projects*
Patents and proprietary rights	*N/A*
Important publications over the last 5 years	*List of current publications:* BLECHOVÁ, Anna, Jakub HARAŠTA and František KASL. From Space Debris to Space Weaponry: A Legal Examination of Space Debris as a Weapon. In C. Kwan, L. Lindström, D. Giovannelli, K. Podinš, D. Štrucl. 2024 16th International Conference on Cyber Conflict: Over the Horizon. 1st ed. Tallinn: NATO CCDCOE Publications, 2024, p. 263-279. ISBN 978-9916-9789-4-8. JAREŠ, Adam, František KASL and Pavel LOUTOCKÝ. Současné výzvy a příležitosti uzavírání smluv online (Current challenges and opportunities for online contracting). Online. Brno: Masarykova univerzita, 2024, 239 pp. Spisy Právnické fakulty Masarykovy univerzity, Edice Scientia, sv. č. 757. ISBN 978-80-280-0523-8. LOUTOCKÝ, Pavel, Miroslav MAREŠ, Jakub DRMOLA, František KASL and Jakub VOSTOUPAL. Cybersecurity Work Force Scarcity - Use Case Czechia: Lessons Learned, Lessons to be Learned. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2024, vol. 2024, March, p. 257-266. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/1cb4ea69-686f-4bcc-9bf5-540c8a3cfe07. VOSTOUPAL, Jakub, Václav STUPKA, Jakub HARAŠTA, František KASL, Pavel LOUTOCKÝ and Kamil MALINKA. The Legal Aspects of Cybersecurity Vulnerability Disclosure: To the NIS 2 and Beyond. Computer Law & Security Review. Great Britain: Elsevier, 2024, vol. 2024, No 53, p. 1-18. ISSN 0267-3649. Available from: https://dx.doi.org/10.1016/j.clsr.2024.105988. KASL, František, Pavel LOUTOCKÝ, Veronika PŘÍBAŇ ŽOLNERČÍKOVÁ, Adam JAREŠ and Martin ERLEBACH. The role of public entities in promoting and regulating the development of the mobility as a service landscape. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2024, vol. 2024, March, p. 233-238. ISSN 1664-848X. MALINKA, Kamil, Anton FIRC, Pavel LOUTOCKÝ, Jakub VOSTOUPAL, Andrej KRIŠTOFÍK and František KASL. Using Real-world Bug Bounty Programs in Secure Coding Course: Experience Report. ArXiv. 2024. Available from: https://dx.doi.org/10.48550/arXiv.2404.12043. KASL, František, Lucie CHMELÍČKOVÁ and Martin ŠVEC. The upcoming Network Code on Cybersecurity and its impact on resilience of the European energy sector. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2024, vol. 2024, March, p. 239-246. ISSN 1664-848X.

	KASL, František and Anna BLECHOVÁ. The road towards a legal framework for cybersecurity applicable to the European smart grid for electricity. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2024, vol. 2024, March, p. 225-232. ISSN 1664-848X. KASL, František, Pavel LOUTOCKÝ and Jakub VOSTOUPAL. The Curation Mechanism for the Czech National Qualifications Framework in Cybersecurity. Online. In Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). New York, NY, USA: Association for Computing Machinery, 2023, p. 1-6. ISBN 979-8-4007-0772-8. Available from: https://dx.doi.org/10.1145/3600160.3605001. OUJEZSKÝ, Václav, Bacem MBAREK, František KASL and Tomáš PITNER. Selected Software and Tools for Smart Grid Simulation in Research. Online. In 2023 15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Belgium: IEEE, 2023, p. 102-106. ISBN 979-8-3503-9329-3. Available from: https://dx.doi.org/10.1109/ICUMT61075.2023.10333271. MAMULA, Ondřej, David HRYCEJ, Tomáš PITNER, František KASL, Martin STŘELEC and Petr JANEČEK. Technology Approaches to Metering in Flexibility Aggregation. Online. In 2023 15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Belgium: IEEE, 2023, p. 122-127. ISBN 979-8-3503-9329-3. Available from: https://dx.doi.org/10.1109/ICUMT61075.2023.10333278. KASL, František, Pavel LOUTOCKÝ, Adam JAREŠ, Veronika PŘÍBAŇ ŽOLNERČÍKOVÁ and Martin ERLEBACH. The regulatory landscape for mobility as a service in a Europe fit for the digital age. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2023, vol. 2023, March, p. 1-8. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/7b84368f-ee19-4b8d-b7df-a1354a47e9ab. BLECHOVÁ, Anna, Jakub DRMOLA, Jan HAJNÝ, František KASL, Pavel LOUTOCKÝ, Miroslav MAREŠ, Tomáš PITNER and Jakub VOSTOUPAL. Mapping Competencies to Cybersecurity Work Roles. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2022, vol. 2022, June, p. 393-400. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/2e2f01cf-ae2c-4536-90ad-460613905754. VOSTOUPAL, Jakub, František KASL, Pavel LOUTOCKÝ, Tomáš PITNER, Patrik VALO, Adam VALALSKÝ and Damián PARANIČ. The Platform for Czech National Qualifications Framework in Cybersecurity. Online. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). New York, NY, USA: Association for Computing Machinery, 2022, p. 1-6. ISBN 978-1-4503-9670-7. Available from: https://dx.doi.org/10.1145/3538969.3543800. PITNER, Tomáš, Václav OUJEZSKÝ, Ondřej MAMULA, František KASL, Martin STŘELEC and Jiří VODRÁŽKA. Comparison of Prevailing Technological Trends in Communication and Control Infrastructure. Online. In 2022 14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Spain: IEEE Computer Society, 2022, p. 159-164. ISBN 979-8-3503-9866-3. Available from: https://dx.doi.org/10.1109/ICUMT57764.2022.9943366. GREGOR, Miloš, Petra MLEJNKOVÁ, Miroslava PAVLÍKOVÁ, Barbora ŠENKÝŘOVÁ, Jakub DRMOLA, Miroslav MAREŠ, František KASL, Aleš HORÁK, Vít BAISA, Radim POLČÁK, Jan HANZELKA, Jonáš SYROVÁTKA and Ondřej HERMAN. Challenging Online Propaganda and Disinformation in the 21st Century. Cham: Palgrave Macmillan, 2021, 273 pp. Political Campaigning and Communication. ISBN 978-3-030-58623-2. Available from: https://dx.doi.org/10.1007/978-3-030-58624-9. KASL, František. Porušení bezpečnosti osobních údajů v kontextu internetu věcí (Personal Data Breach in the Context of the Internet of Things). 1st ed. Brno: Masarykova univerzita, 2021, 346 pp. Spisy Právnické fakulty Masarykovy univerzity, Edice Scientia, sv. č. 717. ISBN 978-80-210-9985-2. HAJNÝ, Jan, František KASL, Pavel LOUTOCKÝ, Miroslav MAREŠ and Tomáš PITNER. Progress towards Czech National Cybersecurity Qualifications Framework. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2021, vol. 2021, 27. Mai, p. 257-262. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/f79f430a-ca8b-409f-9a1f-66135b8ff2d8. HARAŠTA, Jakub, Terezie SMEJKALOVÁ, Tereza NOVOTNÁ, Jaromír ŠAVELKA, Radim POLČÁK, František KASL, Pavel LOUTOCKÝ and Jakub MÍŠEK. Citační analýza judikatury (Citation Analysis of Case Law). 1. vydání. Praha: Wolters Kluwer, 2021. 256 pp. Právní monografie. ISBN 978-80-7598-749-5. MÍŠEK, Jakub, František KASL and Pavel LOUTOCKÝ. Czech Republic: Personal Data Protection Law. European Data Protection Law Review. Berlin: Lexxion, 2020, vol. 6, No 2, p. 289-293. ISSN 2364-2831. doi:10.21552/edpl/2020/2/15. *Full list of publications available here: https://www.muni.cz/en/people/462266-frantisek-kasl/publications*

Activities in specialist bodies over the last 5 years	*Editor-in-Chief (10/2022 - present), Deputy Editor-in-Chief (1/2017-10/2022) - academic journal Revue pro právo a technologie (Review of Law and Technology)* *International Research Fellow (10/2023 - present) - ISLC - Information Society Law Center, Milano, Italia* *Rapporteur of the High Level Expert Group of the European Centre of Excellence for Artificial Intelligence on the non-public draft of the Council of Europe Convention on Artificial Intelligence on Human Rights, Democracy and the Rule of Law (2022)*

Name	*Pavel Loutocký*		
Post	*Lawyer, Head of the section, Post-doc Researcher and Lecturer*		
Academic career	***Ph.D.*** *- (Law of information and communication technologies, intern Ph.D. studies, final thesis "Enforceability of Law through out-of-court Online Dispute Resolution", marked A)*	*Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic*	*2019*
	JUDr. *- (Law of Information and Communication technologies)*	*Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic*	*2017*
	BA (Hons) *– (European Business Law, final thesis focused on out-of-court dispute settlement online)*	*University of Abertay Dundee, Scotland, United Kingdom*	*2011*
Employment	*Lawyer, head of the section, researcher*	*Centre for Education, Research and Innovation in Information and Communication Technologies-ExecUnit, Faculty of Informatics, Masarykova univerzita, Žerotínovo náměstí 9, 601 77 Brno, Czech Republic*	*08/2019 – present*
	Lecturer		*2018 - present*

	Post-doc researcher	*Faculty of Electrical Engineering and Communication Technologies, Brno University of Technology, Technická 3058/10, 616 00 Brno, Czech Republic* *Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic*	*2019 - present*
Research and development projects over the last 5 years	*Selected projects:* *I-tools to Design and Enhance Access to justice (101160528)* *RES-Q Registry for Stroke Care Quality upgrade for stroke care improvement (101057603)* *Capacity building in cybersecurity (VJ03030052)* *Data Flow Protection in Shared Transport Vehicles (CK03000040)* *Sector Skills Alliances 2020 (621701-EPP-1-2020-1-LT-EPPKA2-SSA-B)* *Online dispute resolution (ODR) - conceptual analysis of the feasibility of building an online court/online justice system (TL03000403)* *National Qualification Framework in Cybersecurity (VI20192022161)* *Legal and Technical Means to Protect Privacy in Cyberspace (TL02000398)* *Full list of projects including description available here: https://www.muni.cz/en/people/210290-pavel-loutocky/projects*		
Industry collaborations over the last 5 years	*Selected projects:* *Cybersecurity Innovation Hub (101083932)* *DP16_Cybersecurity Vulnerability Disclosure and Related Procedures (Bugbounty) (MUNI/33/DP16/2021)* *DP10_Compliance Programme for SMEs (MUNI/33/DP10/2020)* *Full list of projects including description available here: https://www.muni.cz/en/people/210290-pavel-loutocky/projects*		
Patents and proprietary rights	*N/A*		
Important publications over the last 5 years	*List of current publications:* JAREŠ, Adam, František KASL and Pavel LOUTOCKÝ. Současné výzvy a příležitosti uzavírání smluv online (Current challenges and opportunities for online contracting). Online. Brno: Masarykova univerzita, 2024, 239 pp. Spisy Právnické fakulty Masarykovy univerzity, Edice Scientia, sv. č. 757. ISBN 978-80-280-0523-8. LOUTOCKÝ, Pavel, Miroslav MAREŠ, Jakub DRMOLA, František KASL and Jakub VOSTOUPAL. Cybersecurity Work Force Scarcity - Use Case Czechia: Lessons Learned, Lessons to be Learned. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2024, vol. 2024, March, p. 257-266. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/1cb4ea69-686f-4bcc-9bf5-540c8a3cfe07. KRIŠTOFÍK, Andrej and Pavel LOUTOCKÝ. ODR and Online courts: What is their future after the AI Act. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2024, vol. 27, No 1, p. 197 - 204. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/9375d02d-afd2-47fd-9e71-ba679710f15a. VOSTOUPAL, Jakub, Václav STUPKA, Jakub HARAŠTA, František KASL, Pavel LOUTOCKÝ and Kamil MALINKA. The Legal Aspects of Cybersecurity Vulnerability Disclosure: To the NIS 2 and		

	Beyond. Computer Law & Security Review. Great Britain: Elsevier, 2024, vol. 2024, No 53, p. 1-18. ISSN 0267-3649. Available from: https://dx.doi.org/10.1016/j.clsr.2024.105988. KASL, František, Pavel LOUTOCKÝ, Veronika PŘÍBAŇ ŽOLNERČÍKOVÁ, Adam JAREŠ and Martin ERLEBACH. The role of public entities in promoting and regulating the development of the mobility as a service landscape. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2024, vol. 2024, March, p. 233-238. ISSN 1664-848X. MALINKA, Kamil, Anton FIRC, Pavel LOUTOCKÝ, Jakub VOSTOUPAL, Andrej KRIŠTOFÍK and František KASL. Using Real-world Bug Bounty Programs in Secure Coding Course: Experience Report. ArXiv. 2024. Available from: https://dx.doi.org/10.48550/arXiv.2404.12043. KASL, František, Pavel LOUTOCKÝ and Jakub VOSTOUPAL. The Curation Mechanism for the Czech National Qualifications Framework in Cybersecurity. Online. In Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). New York, NY, USA: Association for Computing Machinery, 2023, p. 1-6. ISBN 979-8-4007-0772-8. Available from: https://dx.doi.org/10.1145/3600160.3605001. STUPKA, Václav, Jakub VOSTOUPAL and Pavel LOUTOCKÝ. EU – US comparison of approaches to cybersecurity certification and standardization. Jusletter IT. Weblaw AG, 2023, vol. 2023, No 3, p. 427-436. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/f6181a06-5514-4cfb-927a-b695b6ee4dfa. STUPKA, Václav, Pavel LOUTOCKÝ, Antonín DUFKA and Petr ŠVENDA. Multi party signatures and electronic evidence in criminal proceedings. Jusletter IT. Weblaw AG, 2023, vol. 2023, No 3, p. 419-425. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/95440eb4-0311-40e8-80e8-e7761ac25706. KASL, František, Pavel LOUTOCKÝ, Adam JAREŠ, Veronika PŘÍBAŇ ŽOLNERČÍKOVÁ and Martin ERLEBACH. The regulatory landscape for mobility as a service in a Europe fit for the digital age. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2023, vol. 2023, March, p. 1-8. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/7b84368f-ee19-4b8d-b7df-a1354a47e9ab. BLECHOVÁ, Anna, Jakub DRMOLA, Jan HAJNÝ, František KASL, Pavel LOUTOCKÝ, Miroslav MAREŠ, Tomáš PITNER and Jakub VOSTOUPAL. Mapping Competencies to Cybersecurity Work Roles. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2022, vol. 2022, June, p. 393-400. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/2e2f01cf-ae2c-4536-90ad-460613905754. VOSTOUPAL, Jakub, František KASL, Pavel LOUTOCKÝ, Tomáš PITNER, Patrik VALO, Adam VALALSKÝ and Damián PARANIČ. The Platform for Czech National Qualifications Framework in Cybersecurity. Online. In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22). New York, NY, USA: Association for Computing Machinery, 2022, p. 1-6. ISBN 978-1-4503-9670-7. Available from: https://dx.doi.org/10.1145/3538969.3543800. LOUTOCKÝ, Pavel. Possible Approaches towards the Architecture of Online Courts and their Potential in the Decision-making Process. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2022, Neuvedeno, No 5, p. 215-225. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/f37d20de-4f8c-4421-afaa-0d914636f226. HAJNÝ, Jan, František KASL, Pavel LOUTOCKÝ, Miroslav MAREŠ and Tomáš PITNER. Progress towards Czech National Cybersecurity Qualifications Framework. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2021, vol. 2021, 27. Mai, p. 257-262. ISSN 1664-848X. Available from: https://dx.doi.org/10.38023/f79f430a-ca8b-409f-9a1f-66135b8ff2d8. LOEBL, Zbyněk, Pavel LOUTOCKÝ, Martin MAISNER, Michal MATĚJKA, Radim POLČÁK and Marína URBÁNIKOVÁ. Online soudnictví v České republice (Online Justice in the Czech Republic). 1st ed. Praha: Wolters Kluwer, 2021. 146 pp. Právní monografie. ISBN 978-80-7676-131-5. HARAŠTA, Jakub, Terezie SMEJKALOVÁ, Tereza NOVOTNÁ, Jaromír ŠAVELKA, Radim POLČÁK, František KASL, Pavel LOUTOCKÝ and Jakub MÍŠEK. Citační analýza judikatury (Citation Analysis of Case Law). 1. vydání. Praha: Wolters Kluwer, 2021. 256 pp. Právní monografie. ISBN 978-80-7598-749-5. LOUTOCKÝ, Pavel. Vymahatelnost práva pomocí online řešení sporů (Enforcement of Law Through Online Dispute Resolution). 1st ed. Praha: Woltes Kluwer, 2020. 217 pp. Právní monografie. ISBN 978-80-7598-752-5. MÍŠEK, Jakub, František KASL and Pavel LOUTOCKÝ. Czech Republic: Personal Data Protection Law. European Data Protection Law Review. Berlin: Lexxion, 2020, vol. 6, No 2, p. 289-293. ISSN 2364-2831. doi:10.21552/edpl/2020/2/15. LOUTOCKÝ, Pavel. Online Dispute Resolution as an Inspiration for Contemporary Justice. In Schveighofer, E., Kummer, F., Saarenpää (eds.). Internet of Things. Proceedings of the 22th International Legal Informatics Symposium IRIS 2019. Bern: Editions Weblaw, 2019. p. 443-451. ISBN 978-3-96443-724-2.

	Full list of publications available here: https://www.muni.cz/en/people/210290-pavel-loutocky/publications
Activities in specialist bodies over the last 5 years	*United Nations Commission on International Trade Law - observer, Working Group III and IV* *Member if ICANN NextGen* *Chair of section at Cyberspace Conference, Czech Law and IT conference, ARES*

Name	*Lisa J. Moravek*		
Post	*Cybersecurity Teaching Area, Project Coordinator*		
Academic career	*Project Coordinator*	*Brno University of Technology*	*2022-present*
	EU grant/scholarship for certificate studies in Diaspora Studies	*University of the Fraser Valley, Abbortsford Canada*	*2012*
	Master of Education (M.A.) in Biology and English	*University of Muenster, Germany*	*2012*
Employment	*Position*	*Employer*	*Period*
	Teacher of English language	*Grammar school Bystrc, Brno, Czech Republic*	*2023-2024*
	Teacher of English and Biology	*Goerdeler Grammar School, Paderborn, Germany*	*2020-2022*
	Freelance language coach and lecturer	*Brno, Czech Republic*	*2013-2020*
Research and development projects over the last 5 years	1. *2023-2027 – Digital Europe – Digital4Security: European Masters Programme in Cybersecurity and Data Sovereignty*		

	2. *2023 – 2025 - VD182309001 – SKILLS2: Developing international partnerships in education and training of Cybersecurity* 3. *2022-2026 – Horizon Europe – CHESS – Cyber-Security Excellence Hub in Estonia and South Moravia*
Industry collaborations over the last 5 years	*NA*
Patents and proprietary rights	*NA* *Year*
Important publications over the last 5 years	*NA*
Activities in specialist bodies over the last 5 years	*NA*

Name	*Sara Ricci*		
Post	*Post-Quantum Cryptography, Privacy-enhancing Technology, Data Privacy*		
Academic career	*Postdoctoral researcher*	*Brno University of Technology*	*2018-present*
	Postdoctoral researcher	*Universitat Rovira I Virgili, Spain*	*2018*
	FPI grant (PhD program funded by Spanish Government) in Computer Engineering and Mathematics Security	*Universitat Rovira I Virgili, Spain*	*2018* *2015*
	Laurea Magistrale (MSc) in Mathematics	*University of Pisa, Italy*	

Employment	*Position* *Employer* *Period*
Research and development projects over the last 5 years	1. *2023-2027 - Erasmus+ - EULiST **Academic Ecosystem*** 2. *2021 – 2025 - VJ01010008 - NESPOQ: Network Cybersecurity in Post-Quantum Era* 3. *2022-2023 - ERASMUS Lump Sum Grant – DJM-CYBER* 4. *2021-2022 - VJ01030001 - PP3: International Partnership for Cybersecurity Skills Training* 5. *2020-2024 - ERASMUS+: REWIRE - Cybersecurity Skills Alliance - A New Vision for Europe* 6. *2019-2021 - Horizon H2020: 830892 - SPARTA: Special projects for advanced research and technology in Europe* 7. *2019-2021 - TACR: TJ02000290 - Hardware accelerated system with cryptographic security for transferring big data* 8. *2018-2022 - MVCR: Vl20192022126 - Modular hardware accelerator for cryptographic operations*
Industry collaborations over the last 5 years	*NA*
Patents and proprietary rights	*NA* *Year*
Important publications over the last 5 years	• *Ricci S, Dobias P, Malina L, Hajny J, Jedlicka P.:Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. IEEE Access (2024).* • *Ricci S, Parker S, Jerabek J, Danidou Y, Chatzopoulou A, Badonnel R, Lendak I, Janout V.: Understanding Cybersecurity Education Gaps in Europe. IEEE Transactions on Education (2024) .* • *Dzurenda P, Ricci S, Sikora M, Stejskal M, Lendák I, Adão P. Enhancing Cybersecurity Curriculum Development: AI-Driven Mapping and Optimization Techniques. InProceedings of the 19th International Conference on Availability, Reliability and Security (2024).* • *Ricci S, Shapoval V, Dzurenda P, Roenne P, Oupicky J, Malina L. Lattice-based Multisignature Optimization for RAM Constrained Devices. InProceedings of the 19th*

	International Conference on Availability, Reliability and Security (2024). • *Dzurenda P, Ricci S, Ilgner P, Malina L, AnglÄ¨s-Tafalla C.: Privacy-Preserving Solution for European Union Digital Vaccine Certificates. Applied Sciences (2023).* • *Briones Delgado A, Ricci S, Chatzopoulou A, Cegan J, Dzurenda P, Koutoudis I. Enhancing Cybersecurity Education in Europe: The REWIRE's Course Selection Methodology. In Proceedings of the 18th International Conference on Availability, Reliability and Security 2023 (2023)* • *Danidou Y, Ricci S, Skarmeta A, Hosek J, Zanero S, Lendak I. DJM-CYBER: A Joint Master in Advanced Cybersecurity. In Proceedings of the 18th International Conference on Availability, Reliability and Security 2023 (2023)* • *Ricci, S., Dzurenda, P., Hajny, J., Malina, L.: Privacy-Enhancing Group Signcryption Scheme. IEEE Access (2021).* • *Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., De Nicola, R.: Framework, Tools and Good Practices for Cybersecurity Curricula. IEEE Access (2021).* • *Farras, O., Ribes-Gonzalez, J., Ricci, S.: Privacy-preserving data splitting: a combinatorial approach. Designs, Codes and Cryptography (2021).* • *Malina, L., Dzurenda, P, Ricci S., Hajny, J., Srivastava, G., MatuleviÄŤius, R.,* • *Abasi-amefon, O.A., Laurent, M., Sultan, N.H., Tang, Q.: Post-Quantum Era Privacy Protection for Intelligent Infrastructures. IEEE Access (2021).* • *Domingo-Ferrer, J., Sanchez, D., Ricci, S., Muñoz-Batista, M: Outsourcing analyses on privacy-protected multivariate categorical data stored in untrusted clouds. In Knowledge and Information Systems (2020).*
Activities in specialist bodies over the last 5 years	*Women4Cyber Mentor 2024-present* *Membership without a specific role need not be mentioned*

Name	*Vaclav Stupka*		
Post	*Deputy director, Cybersecurity law, governance and compliance*		
Academic career	***Ph.D.*** *- Law of information and communication technologies, final thesis "Cybersecurity law", marked A)*	*Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic*	*2018*
	MA - *Law of Information and Communication technologies*	*Institute of Law and Technology, Faculty of Law, Masaryk University, Brno, Czech Republic*	*2010*
Employment	*Deputy director*	*Cybersecurity Hub, z.ú., Šumavská 416/15, 602 00, Brno, Czech Republic*	*2021 – present*
	Lawyer, manager, senior researcher and lecturer	*Faculty of Informatics, Faculty of law,, Masaryk university, Žerotínovo náměstí 9, 601 77 Brno, Czech Republic*	*2013 – present*
	Lecturer		*2018 - present*
	Lawyer, IT manager	*Faculty of Electrical Engineering and Communication Technologies, Brno University of Technology, Technická 3058/10, 616 00 Brno, Czech Republic*	*2011 - 2013*
		LAC, s.r.o. Štefánikova,	

	Rajhrad, Czech Republic
Research and development projects over the last 5 years	*Selected projects:* *2023 – CURRENT* ***National Coordination Centre - NCC-CZ*** *Lead of the CyberSecurity Hub project team. Total Budget for this run of the project is € 1 million. https://ncc.nukib.cz/* *2023 – CURRENT* ***Cyber-security Excellence Hub in Estonia and South Moravia (CHESS)*** *Lead of the CyberSecurity Hub project team. The total budget of the project is € 5 million. https://chesseu. cs.ut.ee/about/* *2023 – CURRENT* ***RES-Q+ Comprehensive solution of healthcare improvement based on the global Registry of Stroke Care Quality*** *Lead of the Masaryk University proejct team. Total Budget of the project is € 8 million. https://www.resqplus.eu/* *2021 – CURRENT* ***Electronic Evidence in Criminal Proceedings (VJ01010084)*** *Principal investigator and lead of the project team. Project budget € 2 million.* *2020 – CURRENT* ***The Cybersecurity Skills Alliance – New Vision for Europe – REWIRE*** *(621701-EPP-1-2020-1-LT-EPPKA2- SSA-B) Lead of the Masaryk University project team. Project budget € 4 million. https://www.rewireproject.eu* *2018 – 2023* ***CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence*** *(CZ. 02.1.01/0.0/0.0/16_019/0000822) Senior researcher in the legal team. Project budget € 10 million. https://www.c4e.cz* *2019 – 2023* ***National Cybersecurity Competence Centre*** *(TN01000077) As a legal specialist, I participated mainly in projects focused on*

	certification in cyber security, implementation of network surveillance and SOC tools, vulnerability disclosure, and the development of educational tools and cyber security exercises. As deputy director, I am responsible for coordinating cooperation between research organizations and companies involved in sub-projects. Project budget € 5 million. https://www.nc3.cz *2016 – 2019* ***The Sharing and Analysis of Security Events in the Czech Republic** (VI20162019029) Legal lead of the project - my team focused on the design of the information-sharing mechanisms of the system to comply with cybersecurity and privacy regulations. https://sabu.cesnet.cz/en* *2016 – 2019* ***Criminal Justice Access to Digital Evidences in the Cloud - LIVE_FORensics** (723150) Lead of the project team at Masaryk - responsible for deployment of trainings. http://live-for.eu* *2016 – 2019* ***Simulation, Detection, and Mitigation of Cyber Threats Endangering Critical Infrastructure** (KYPO II) Legal lead in the project and also in development of training scenarios. https://www.kypo.cz* *2014 – 2020 **Cyber Czech Security Exercise Cyber Czech** Legal lead - involved in development of training scenarios as well as in deployment of the trainings. https://csirt.muni.cz/projects/cyber-czech*
Industry collaborations over the last 5 years	*Selected projects:* *Cybersecurity Innovation Hub (101083932)* *DP16_Cybersecurity Vulnerability Disclosure and Related Procedures (Bugbounty) (MUNI/33/DP16/2021)* *DP10_Compliance Programme for SMEs (MUNI/33/DP10/2020)* *Full list of projects including description available here:* *https://www.muni.cz/en/people/210290-pavel-loutocky/projects*
Patents and proprietary rights	*N/A*
Important publications over the last 5 years	*Selected publications:* *VOSTOUPAL, Jakub, Václav STUPKA, Jakub HARAŠTA, František KASL, Pavel LOUTOCKÝ a Kamil MALINKA. The Legal Aspects of Cybersecurity Vulnerability Disclosure: To the NIS 2 and Beyond.*

	Computer Law & Security Review. Great Britain: Elsevier, 2024, roč. 2024, č. 53, s. 1-18. ISSN 0267-3649. Dostupné z: https://dx.doi.org/10.1016/j.clsr.2024.105988. *POLČÁK, Radim, Matěj MYŠKA, Petr HOSTAŠ, František KASL, Tereza KYSELOVSKÁ, Tomáš LECHNER, Pavel LOUTOCKÝ, Jakub MÍŠEK, Jan TOMÍŠEK, Václav STUPKA and Miroslav UŘIČAŘ. Právo informačních technologií (Information Technology Law). Praha: Wolters Kluwer, 2019. 656 pp. Právní monografie. ISBN 978-80-7598-045-8.* *SEEBA, Mari, Tarmo OJA, Maria Pibilota MURUMAA and Václav STUPKA. Security level evaluation with F4SLE. In ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security. New York, NY, USA: ACM, 2023. p. 1-8. ISBN 979-8-4007-0772-8. doi: 10.1145/3600160.3605045.* *STUPKA, Václav, Jakub VOSTOUPAL and Pavel LOUTOCKÝ. EU – US comparison of approaches to cybersecurity certification and standardization. Jusletter IT. Weblaw AG, 2023, vol. 2023, No 3, p. 437-436, 10 pp. ISSN 1664-848X. doi:10.38023/f6181a06-5514-4cfb-927a-b695b6ee4dfa.* *STUPKA, Václav a Juraj SZABÓ. Service providers and electronic evidence collection. Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2022, roč. 2022, June, s. 401-407. ISSN 1664-848X. doi: 10.38023/44f4c82a-d2e3-40dd-864f-b620f1b70d1d. SELECTED PUBLICATIONS* *STUPKA, Václav, Jan PROVAZNÍK and Jakub VOSTOUPAL. Elektronické důkazy jako výzva pro trestní proces (Electronic Evidence as a Challenge to Criminal Proceedings). Právník. AV ČR, Ústav státu a práva, 2022, No 4, 17 pp. ISSN 0231-6625.* *MICHOTA, Alexandra, Václav STUPKA, Andreas MITRAKAS, Andreas SFAKIANAKIS, Catalin PATRASCU, François BEAUVOIS, Koen VAN IMPE, Silvia SIGNORATO and Smaragda KARKALA. Roadmap on the cooperation between CSIRTs and LE. Greece: European Union Agency for Cybersecurity, 2020. ISBN 978-92-9204-331-5. doi:10.2824/40199.* *STUPKA, Václav and Jakub VOSTOUPAL. Evropský certifikační rámec kyberbezpečnosti ICT produktů, služeb a procesů (The European Cybersecurity Certification Framework for Products,*

	Services and Processes). Data Security Management. Praha: TATE International s.r.o., 2020, vol. 24, No 2, p. 25-29. ISSN 1211-8737. *HORÁK, Martin, Václav STUPKA and Martin HUSÁK. GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019). New York: ACM, 2019. p. "36:1"-"36:8", 8 pp. ISBN 978-1-4503-7164-3. doi:10.1145/3339252.3340516.* *STUPKA, Václav, Martin HORÁK a Martin HUSÁK. Protection of personal data in security alert sharing platforms. In Proceedings of the 12th International Conference on Availability, Reliability and Security. Reggio Calabria: ACM, 2017. s. "65:1"-"65:8", 8 s. ISBN 978-1-4503-5257-4. doi: 10.1145/3098954.3105822.* *STUPKA, Václav. Analýza datového provozu jako prevence kybernetických bezpečnostních incidentů (Analysis of data traffic as a cyber security incidents prevention). Data Security Management, Praha: TATE International s.r.o., 2016, vol. 2016, No 3, p. 44-48. ISSN 1211-8737.* *Full list here: https://www.muni.cz/en/people/134455-vaclav-stupka/publications*

Activities in specialist bodies over the last 5 years	*Organisation*	*Role*	*Period*
	ENISA	*Member of the Stakeholder cybersecurity certification group and listed expert*	*2017 – current*
	Ministry of Justice of the Czech Republic	*Member of expert group on digital evidence*	*2016 – current*
	Ministry of Foreign Affairs of the Czech Republic	*CyberVAC project tema member, member of cybersecurity capacity building team*	*2022 – current*
	National Cyber and Information Security Agency	*Member of NCC-CZ advisory group, advisor*	*2020 - current*

Munster Technological University

Name	*Gillian O'Carroll*		
Post	*Cybersecurity Lecturer – Governance, Risk & Compliance*		
Academic career	*Initial academic appointment*	*Munster Technological University*	*2022*
	Habilitation *[German post-doctoral qualification] (subject)*	*n/a*	
	Doctorate (subject)	*n/a*	
	Undergraduate degree (subject)	*Bachelor of Commerce*	*1996*
		University College Cork	*2010*
		MBS Corporate Finance & Accounting, UCC	
Employment	*Position*	*Employer*	*Period*
	Risk Manager	*First South Credit Union*	*2019 – 2022*
	Project Manager	*First South Credit Union*	*2016 – 2019*
	Internal Auditor	*First South Credit Union*	*2010 – 2016*
	Audit Manager	*First South Credit Union*	*2007 – 2009*
	Corporate Services Manager	*EY Cork*	*2000 – 2004*
	Auditor	*PwC Cayman Island*	*1996 - 2000*
		EY Cork	
Research and development projects over the last 5 years	*Name of project or research focus: Digital Resilience for Small Businesses*		

	Period and any other information: 2023 to date *Partners, if applicable: Irish National Cyber Security Centre* *Amount of financing: €250,000*
Industry collaborations over the last 5 years	*n/a*
Patents and proprietary rights	*n/a*
Important publications over the last 5 years	*n/a*
Activities in specialist bodies over the last 5 years	*Organisation* *Role* *Period* *n/a*

Vytautas Magnus University

Name	*Prof. dr. Daiva Vitkutė-Adžgauskienė*		
Post	*Teaching in undergraduate and graduate studies at the Faculty of Informatics of Vytautas Magnus University in the field of Computer Science and Digital Transformation (Computer Architecture and Operating Systems, Information Society Technologies, Digital Transformation and ICT Infrastructure, Digitalization and Financial Technologies, Management Information Systems). Her main research interests are in digital transformation processes, natural language processing, semantic technologies and system modelling.*		
Academic career	*Head of Department of Applied Informatics*	*Vytautas Magnus University*	*2021*
	Professor	*Vytautas Magnus University*	*2016*
	Dean, Faculty of Informatics	*Vytautas Magnus University*	*2010*
	Associate Professor	*Vytautas Magnus University*	*1995*
	Researcher	*Vytautas Magnus University*	*1990*
	Researcher	*Vytautas Magnus University*	*1985*
	PhD (Informatics)	*Vytautas Magnus University*	*1994*
	Master of Business Administration, International Executive MBA	*Lithuanian Energy institute*	*2003*
	Diploma of Higher Education (Computer Science)	*Vytautas Magnus University* / *Baltic Management Institute & Vytautas*	*1985*

		Magnus University *Kaunas University of Technology*	
Employment	*Head of Department of Applied Informatics* *Professor* *Dean* *Head of Product Management, Head of Service Development* *Associate Professor* *Researcher* *Researcher*	*Vytautas Magnus University* *Vytautas Magnus University* *Vytautas Magnus University* *JSC "Omnitel", later "Telia"* *Vytautas Magnus University* *Lithuanian Energy Institute (formerly Institute of Physical-Technical Energy Problems)*	*2021-now* *2016-now* *2010-2021* *1995-2009* *1995-2016* *1990-1994* *1985-1990*
Research and development projects over the last 5 years	DIGITAL-ECCC-2022-CYBER-B-03. „Standard Alert Format Exchange for SOCs (SAFE4SoC)", No. 101145846 (2023-2027). Coordinator for project partner (VMU). DIGITAL-2022-SKILLS-03 "European Masters Programme in Cybersecurity Management & Data Sovereignty (Digital4Security)",		

	project No. 101123430 (2023-2027). Coordinator for project partner (VMU). Project No. LT07-1-EIM-K02-016 "Airborne holographic imaging interface" (2022-2023). Development of the National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena (NAAS). Stage II of Pre-Commercial Procurement, run by contracting authorities – General Jonas Žemaitis Military Academy of Lithuania and Mykolas Riomeris University, project No. 01.2.1-LVPA-V-835-03-0006, agreement No. ESIF1-1047 (I stage: 2020-2021; II stage – 2021-2022; III stage – 2023). Project coordinator at VMU. 5.Common Language Resources and Technology Infrastructure, European Research Infrastructure Consortium (CLARIN ERIC) (MTI-02/2015) (2017-2020). Project researcher.
Industry collaborations over the last 5 years	*Project title* *Partners*
Patents and proprietary rights	*Title* *Year*
Important publications over the last 5 years	1. Eligijus Sakalauskas, Antanas Bendoraitis, Dalė Lukšaitė, Gintaras Butkus, Daiva Vitkutė-Adžgauskienė, *Tax Declaration Scheme Using Blockchain Confidential Transactions*, Informatica **34**(2023), no. 3, 603-616, DOI 10.15388/23-INFOR531. 2. Rytis Maskeliunas; Robertas Damaševičius; Daiva Vitkute-Adzgauskiene; Sanjay Misra. Pareto Optimized Large Mask Approach for Effcient and Background Humanoid Shape Removal // IEEE Access, 2023, Vol. 11. Prieiga per Internetą: https://ieeexplore.ieee.org/document/10061219. [Databases: Clarivate Analytics: Science Citation Index (SCI), Scopus, INSPEC]. 3. Mohammed Hasan Ali; Mustafa Musa Jaber; Sura Khalil Abd; Amjad Rehman; Mazhar Javed Awan; Daiva Vitkutė-Adžgauskienė; Robertas Damaševičius; Saeed Ali Bahaj. Harris Hawks Sparse Auto-Encoder Networks for Automatic Speech Recognition System // Appl. Sci. 2022, Volume 12, Issue 3, 1091. Internet access: <https://doi.org/10.3390/app12031091>. [Databases: Clarivate Analytics: Science Citation Index (SCI), Scopus]. 4. Petkevičius, Mindaugas; Vitkutė-Adžgauskienė, Daiva. Intrinsic word embedding model evaluation for Lithuanian language using adapted similarity and relatedness benchmark datasets // CEUR Workshop proceedings IVUS 2021, Kaunas, Lithuania, April 23, 2021, Aachen: CEUR-WS, 2021, Vol. 2915, ISSN 1613-0073, p. 122-131. Internet access: http://ceur-ws.org/Vol-2915/paper14.pdf. 5. Petkevičius, Mažvydas; Vitkutė-Adžgauskienė, Daiva; Amilevičius, Darius. Targeted aspect-based sentiment analysis for Lithuanian social media reviews // Human language technologies - the Baltic perspective : proceedings of the 9th international conference, Baltic HLT, Kaunas, Lithuania, 22-23 September, 2020 / editors Andrius Utka, Jurgita

	Vaičenonienė, Jolanta Kovalevskaitė, Danguolė Kalinauskaitė. Amsterdam: IOS Press, 2020, ISBN 9781643681160. p. 32-38. Internet access: <https:/doi.org/10.3233/FAIA200599>. [Databases: Science Citation Index Expanded (Web of Science)]. 6. Minija Tamosiunaite, Mohamad Javad Aein, Jan Matthias Braun, Tomas Kulvicius, Irena Markievicz, Jurgita Kapociute-Dzikiene, Rita Valteryte, Andrei Haidu, Dimitrios Chrysostomou, Barry Ridge, Tomas Krilavicius, Daiva Vitkute-Adzgauskiene, Michael Beetz, Ole Madsen, Ales Ude, Norbert Krüger, Florentin Wörgötter, "Cut & recombine: reuse of robot action components based on simple language instructions", The International Journal of Robotics Research, 2019, ISSN: 0278-3649, vol 38, Issue 10-11, p. 1179-1207. Internet access: https://journals.sagepub.com/doi/10.1177/0278364919865594. [Databases: Clarivate Analytics: Science Citation Index (SCI), Scopus].		
Activities in specialist bodies over the last 5 years	*Centre for Quality Assessment in Higher Education (Lithuania)*	*Expert*	*2014-now*
	Innovation Agency (formerly Lithuanian Business Support Agency)	*Expert*	*2018-now*
	Quality Agency for Higher Education AIKA (Latvia)	*Expert*	*2023-now*

Digital4Security
Shaping Europe's cyber future

Legal Disclaimer

The European Commission's support to produce this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Project 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03

Digital4Security

Shaping Europe's cyber future

ADVANCED DIGITAL SKILLS

DIGITAL EUROPE PROGRAMME

Co-funded by the European Union

Digital4Security
Shaping Europe's cyber future

Master in Cybersecurity Management & Data Sovereignty

Internal Quality Handbook 2024

Table of Contents

1. Introduction

Digital4Security is a ground-breaking pan-European master's program aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. This €20m industry-led Master's, supported by funding from the DIGITAL Europe Programme, is a four-year initiative that comprises a Consortium of 36 partners spanning 12 countries. This master program will provide comprehensive knowledge of cybersecurity management, regulatory compliance, and technical expertise to European SMEs and companies.

Digital4Security is launching a collective cybersecurity revolution by harnessing the collective skill sets of our international Consortium, and the next generation of practical experts in the digital space. We're reskilling and upskilling graduates, professionals, managers and business leaders to become 'cyber confident', equipped to protect and empower European SMEs in the face of global cyber threats.

The Digital4Security curriculum is grounded in a rigorous needs analysis process involving all of our Consortium partners. The programme will blend academic and industry content to ensure graduates are equipped with both theoretical and job-ready cyber skills to fast-track employment. The program is designed to meet European accreditation standards and a wide range of national standards, with plans to offer micro-credentials for each module and industry certification in collaboration with our industry partners.

2. The Digital4Security Consortium

The Digital4Security Consortium is a dynamic pan-European partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management programme, developed and delivered by the best cybersecurity talent from Europe and worldwide. Table 1 lists the Higher Education Institutions (HEIs) jointly offering the master's degree, while Table 2 presents additional consortium partners, including industry stakeholders.

Table 1: Academic Partners (Higher Education Institutes) Offering the Joint Degree Program

No.	Partner	Abbreviation	Country
1	Universitatea Nationala de Stiinta si Technologies Politehnica Bucuresti	POLITEHNICA B.	Romania
2	National College of Ireland	NCI	Ireland
3	German University of Digital Science gGmbH	UDS	Germany
4	University of Rijeka	UNIRI	Croatia

5	Università degli Studi di Brescia	UNIBS	Italy
6	Politecnico di Milano	POLIMI	Italy
7	Universität Koblenz	UNI KO	Germany
8	CY Cergy Paris Université	CY	France
9	Mykolo Romerio Universitetas	MRU	Lithuania
10	Universidad Internacional de La Rioja	UNIR	Spain
11	Brno University of Technology	BUT	Czech Republic
12	Munster Technological University	MTU	Ireland
13	Vytautas Magnus University	VMU	Lithuania

Table 2: Associate Partners

No.	Associated Partner	Abbreviation	Country
14	DIGITAL TECHNOLOGY SKILLS LIMITED	DTSL	Ireland
15	IT@CORK ASSOCIATION LIMITED LBG	IT@CORK	Ireland
16	SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	SKILLNET	Ireland
17	ADECCO FORMAZIONE SRL	ADECCO TRAINING	Italy
18	ADECCO ITALIA HOLDING DI PARTECIPAZIONE E SERVIZI SPA	ADECCO GROUP	Italy
19	ADECCO ITALIA SPA	Adecco Italia	Italy
20	CEFRIEL SOCIETA CONSORTILE A RESPONSABILITA LIMITATA SOCIETA BENEFIT	CEFRIEL	Italy
21	ATAYA & PARTNERS	Ataya	Belgium
22	CYBER RANGES LTD	Cyber Ranges	Cyprus
23	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	FHG	Germany
24	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	NASK	Poland
25	POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	CMIP	Poland
26	SCHUMAN ASSOCIATES SCRL	SA	Belgium
27	CONTRADER SRL	Contrader	Italy
28	INDEPENDENT PICTURES LIMITED	indiepics	Ireland

29	MATRIX INTERNET APPLICATIONS LIMITED	MATRIX	Ireland
30	PROFIL KLETT D.O.O.	PROFIL KLETT	Croatia
31	SERVICENOW IRELAND LIMITED	ServiceNow	Ireland
32	EUROPEAN DIGITAL SME ALLIANCE	DIGITAL SME	Belgium
33	DIGITALEUROPE AISBL*	DIGITALEUROPE	Belgium
34	TERAWE TECHNOLOGIES LIMITED	TERAWE	Ireland
35	BANCO SANTANDER SA	BANCO SANTANDER /Santander	Spain
36	RED OPEN S.R.L.	RED OPEN S.R.L.	Italy

The HEIs, in conjunction with the Digital4Security consortium's industry partners, have collaborated and cooperated to jointly develop and design this programme and its curriculum.

3. Definitions

Quality assessment procedures in the programme have been agreed by all partners and refer to two different levels:

1. External;
2. Internal.

Quality assessment in the programme has been developed according to the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG) and the European Approach for Quality Assurance of Joint Programmes adopted by the Ministers responsible for higher education in the European Higher Education Area in May 2015. The ESG provide guidance for internal and external quality assurance in higher education.

The European Approach, which is mainly based on the ESG and on the Qualifications Framework for the European Higher Education Area (QF-EHEA), facilitate integrated approaches to quality assurance of joint programmes that genuinely reflect and mirror their joint character.

Digital4Security has taken the standards defined in the European Approach for Quality assurance of Joint Programs and the European Qualifications Framework (EQF) as a basis for its external quality assurance to facilitate an integrated approach to quality assurance.

The Digital4Security Master's degree programme adheres to a transnational internal quality assessment system which is described in this handbook. The Internal Quality Handbook of the Joint Master's Degree in Advanced Digital Skills programme is:

- A permanent roadmap enabling the Quality Enhancement and Curriculum Development taskforce of the degree program, to effectively and efficiently collect data from all identified sources and generate information and proposals for improvement.
- A consistent guideline to develop actions that support the ongoing quality improvement of the degree program coherent set of procedures and tools that combine rigor with simplicity, practicality and flexibility / adaptability.
- A joint initiative that demonstrates that the realization of the master's programme is being monitored in a collaborative way.
- A system that is compatible with and sensitive to variations in national legislations and administrative processes.

3. Quality Policy of the Master's Degree

Each of the Digital4Security partner institutions has been committed within the Bologna process to common standards and guidelines in quality assurance, as a well as a common degree structure and credit system. The programme is modularized to enhance flexibility and meet the demands of target learners.

Mobility is an integral part of the Digital4Security teaching-learning process. For students, in the main, this is a virtual mobility due to the fully online programme delivery.

The programme is assessed based on jointly agreed learning outcomes built around the profile (theoretical knowledge and practical skills) required of advanced digital skills professionals which requires a solid knowledge and understanding of current technological advances and how these technologies may be used for innovative and transformative purposes within business.

The content of the modules, their layout and the complementary capacity building and problems solving activities aim to provide the required knowledge and skills in a complex technological landscape and within an international learning framework respecting and taking advantage of the different contextual backgrounds and variety of expertise in the Digital4Security partner institutions.

The programme incorporates a jointly designed and fully integrated academic curriculum. To achieve the programme learning outcomes, learners must obtain 120 ECTS.

The programme comprises 9 mandatory and a suite of 14 elective modules. The modules cover topics such as:

Nr.	Module	Mand. / Elect.	ECTS
1	AI & Emerging Topics in Cybersecurity	Mandatory	10
2	Business Resilience, Incident Management and Threat Response	Mandatory	10
3	Cybersecurity Culture, Strategy & Leadership	Mandatory	10

Nr.	Module	Mand. / Elect.	ECTS
4	Dissertation / Internship	Mandatory	25
5	Enterprise Architecture, Infrastructure Design and Cloud Computing	Mandatory	10
6	Law, Compliance, Governance, Policy, and Ethics	Mandatory	10
7	Research Methods	Mandatory	5
8	Security Operations	Mandatory	10
9	Technological Foundations for CS & Security Controls	Mandatory	10
10	Automation of Security Tasks and Data Analytics	Elective	5
11	CISO and Crisis Communication	Elective	5
12	Risk Management of Cyber-Physical Systems	Elective	5
13	Cybersecurity Auditing	Elective	5
14	Cybersecurity Economics & Supply Chain	Elective	5
15	Cybersecurity Education & Training Delivery I	Elective	5
16	Cybersecurity Education & Training Delivery II	Elective	5
17	Cybersecurity in Industry - Security of OT and Cyber-Physical Systems	Elective	5
18	Cybersecurity Law & Data Sovereignty	Elective	5
19	Machine and Deep Learning in Cybersecurity	Elective	5
20	Digital Forensics, Chain of Custody and eDiscovery	Elective	5
21	Ethical Hacking & Penetration Testing	Elective	5
22	Malware Analysis	Elective	5
23	Threat Intelligence	Elective	5

The degree programme is integrated within the degree catalogues of each partner institution. The use of ECTS by all partners in Europe and as a reference outside Europe makes it easier to create and document learning pathways, thus allowing better flexibility and comparability.

Entry requirements and admission criteria for the Digital4Security programme are common for all students. They will be rendered available alongside the application procedure on the Digital4Security website at https://www.Digital4Security.eu. Additionally, the partnership consortium has adopted common study and examination rules and regulations. The joint aspects of the programme design and delivery also extend to:

- Jointly developed and shared quality assurance mechanisms: Quality assessment procedures have been agreed by all partners and refer to two different levels, i.e., external and internal.

- Joint governance and joint administrative and financial management: The consortium partnership has an agreed structure for the joint delivery of the programme. This is based on the Cooperation Agreement for the governing and the implementation of the Joint Master's Degree in Advanced Digital Skills.
- Joint Degree Award: According to the Cooperation Agreement, each student who successfully completes the degree programme as described in the Study and Examination Regulations and who has fulfilled the requirements of the applicable national legislations shall receive a joint Master's degree testified by a joint diploma on behalf of the degree awarding Partner Institutions involved in the provision of the degree programme to that student.

The Digital4Security European Joint Master's Degree in Advanced Digital Skills consortium aims to design and implement a highly innovative, effective, and sustainable European EQF Level 7 programme in Advanced Digital Skills. This contributes to the overall objectives of the DIGITAL Europe Programme by fast-tracking a high number of graduates through a dynamic pan-European stakeholder ecosystem. In the latter, HEIs, Research Centres, Employment Services, and Industry work together to design, promote, deliver and improve an innovative Master's programme. It will focus on the practical application of Advanced Digital Skills within European Business, an entirely market-led academic programme driven and designed to meet the current and future (up)-skill needs of SMEs and Companies.

5. Digital4Security Master's Governance and Management Structure

The Master's degree programme has the following management structures defined with responsibilities of decision, of evaluation and execution:

5.1. Roles and Duties

A. Programme Directors: Each Partner Institution appoints at least one academic Programme Director. The Programme Director shall liaise with his or her counterparts in the other Partner Institutions on all matters concerning the degree programme and shall ensure that the degree programme at his or her Partner Institution is consistent with the joint agreements concerning the degree programme.

B. Programme Coordinators: The Programme Coordinator assists the Programme Director and carries out day-to-day administrative and technical tasks concerning the students, quality assurance, mobility in the degree programme and general matters related to programme delivery by the partner institutions. He or she liaises with the other Partner Institution Programme Coordinators and Programme Directors, students in the degree programme, and with external partners. In addition, the Programme Coordinators support the Secretariat and the Joint Programme Committee, as defined in Section 4.2.2 and Section 4.2.5 respectively, with the data collection system, information analysis and proposals and suggestions for the quality enhancement of the Master.

C. Programme Faculty: The academic teaching staff of the Partner Institutions and associated partners directly involved in the development and implementation of the degree programme.

D. Issuing Institution: The degree-awarding Partner Institution responsible for the issuing of the physical joint degree award, its diploma supplement, and any pertaining tasks on behalf of or in joint decision with the other degree-awarding Partner Institutions and non-degree-awarding Partner Institutions as described in this Agreement. The development of formal documentation relating to the joint degree award, the parchment, diploma supplement and any other formal documentation relating to the joint Master's degree programme shall be undertaken in consultation with, and subject to formal approval by, the Partner Institutions.

E. Project Coordinator: The Coordinator UNSTPB is responsible for:

- Student Recruitment, Onboarding, and Support: Managing recruitment, onboarding, and support processes, including the use of digital platforms and supplementary events.
- Industry Certifications & Micro-Credentials: Implementing industry certifications and micro-credentials.
- Employability Programme: Establishing an employability programme for students.
- European Mobility Programme: Facilitating student and lecturer mobility between institutions and companies.
- Faculty Training Resources: Providing resources for faculty training and support.

5.2. Joint Governing Bodies

All governing bodies established by this Agreement and herein described which have responsibility for the various aspects of the joint Master's degree programme, shall be subject to the internal governance and management arrangements and oversight of the respective Partner Institutions. The following governing bodies are established:

- Master's Board of Directors,
- the Secretariat,
- the Project Coordinator
- the Joint Admissions Board,
- the Examination Board,
- the Joint Programme Committee,
- the Quality Enhancement and Curriculum Development Committee,
- and when required, ad hoc committees.

5.2.1 Programme Board of Directors

A. The Programme Board of Directors, hereinafter the Master's Board, shall comprise the Programme Directors that have been selected by each of the Partner Institutions to represent them on all matters concerning the degree programme within the limits of this Agreement. The Master's Board shall be responsible for general management, financial supervision, academic supervision, quality assurance, degree awarding and recognition issues, agreement changes, dispute resolution and student complaints. Additionally, the Master's Board is responsible for the

system review, advice on policy developments for the joint degree programme, and to ensure the coherence and consistency of the concept of the programme.

B. The Programme Director of each Partner Institution shall be a voting member on the Master's Board.

C. The Master's Board establishes by consensus its own decision-making procedures and for which domains consensus shall not be required, unless stated otherwise in this cooperation agreement.

D. The Master's Board shall meet at least twice each year. Meetings may either be in person or held via electronically mediated systems or a combination of in person / electronically mediated.

E. In case of absence, a Programme Director should mandate a deputy to replace and represent him or her as a voting member in meetings of the Master's Board.

F. Minutes of the Master's Board meeting shall be distributed to all members of the Master's Board within fifteen days after the meeting. Any changes to the draft minutes must reach the Programme Secretariat within one week after the distribution of the minutes. After this deadline, the Programme Secretariat shall produce and file a final version, a copy of which shall also be sent to all Programme Directors.

5.2.2 Programme Secretariat

A. The Secretariat shall have the responsibility for the overall daily operational and administrative management of the programme under the guidance and governance of the Master's Board.

B. The Secretariat shall be partly based at the Project Coordinator Institution, also designated as the Master's Secretariat, to support the coordination and day-to-day management of the programme and its support mechanisms, specifically tasks regarding quality assurance, application, selection and admission, student administration, and mobility coordination.

C. The Secretariat shall also include a wider group of Programme Coordinators (as detailed in Section 4.1/B). Each Partner Institution shall designate a representative member to serve on the Programme Coordinators group. These institutional representatives will collaborate with their counterparts from other partner institutions. They will provide administrative support to the Secretariat, addressing issues specifically related to the partner institution they represent.

D. The Secretariat shall also provide direct assistance for the Master's Board Meetings (including the preparation of minutes), maintaining the public website, and performing additional duties as delegated by the Master's Board.

5.2.3 Joint Admissions Board

A. Assisted by the Secretariat and under the supervision of the Master's Board, the Joint Admissions Board shall be responsible for the selection and admission of all students to the degree programme.

B. The Joint Admissions Board shall consist of one representative from each Partner Institution. The Partner Institution is responsible for appointing its representative in accordance with its own procedures and national regulations.

C. The Joint Admissions Board convenes physically or through electronically mediated systems at least once after each application deadline and can hold additional meetings until a selection and admission procedure is completed.

5.2.4 Examinations Board

A. The Examinations Board is headed by the Master's Board of Directors. The Master's Board is responsible for the overall quality and standards of the degree programme and for agreeing upon the academic standards. It monitors the partner institutions' compliance and is responsible for the degree programme being delivered to the highest academic standards.

B. The Examinations Board may be supplemented with additional nominees from Partner Institutions that have expertise in quality assurance and those who are responsible for programme examination administration.

C. Meetings of the Examinations Board shall convene after each programme examination session and after a provision of adequate time for grading and assessment of learners' exam scripts, project submissions, or other relevant coursework by programme faculty.

D. The Examinations Board shall deliberate cases, brought to its attention with at least one week notice. If the nature of the case brought to its attention demands a swift ruling, a special meeting may be arranged or written consultation of its members via electronically mediated systems instead.

E. All assessments are conducted in accordance with the jointly agreed policies and procedures for the degree programme as adopted by the Master's Board.

5.2.5 Joint Programme Committee

A. The Joint Programme Committee acts as advisor to the Master's Board of Directors. It is responsible for the system review and advice on policy developments for the joint degree programme.

B. The Joint Programme Committee meets physically and/or via electronically mediated systems at least once a year to ensure the coherence and consistency of the concept of the joint degree

programme. Additional meetings, including those specified by the Handbook of the programme, can be held when appropriate.

C. The Joint Programme Committee is composed of representatives from the Secretariat, Programme Coordinators, the Master's Board of Directors, and Faculty representatives.

5.2.6 Quality Enhancement and Curriculum Development Committee

A. The Quality Enhancement and Curriculum Development Committee, hereinafter the QECD Committee, is composed of at least one academic faculty member from each Partner Institution.

B. The QECD Committee prepares and implements on behalf of the Master's Board of Directors quality enhancement and curriculum development and reinforces the jointness of the degree programme adhering to the European Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG). The QECD Committee is accountable to the Master's Board.

C. The QECD Committee meets whenever called upon or whenever the periodic internal quality procedures as detailed in the Internal Quality Handbook of the Programme require, either in person or via electronically mediated systems.

D. The QECD Committee assists the Joint Programme Committee to evaluate the degree of achievement of learning objectives and the coherence of the programme and ensures that there are effective procedures for data collection, information analysis and proposals and the channeling of suggestions for improvement of the degree programme.

5.2.7 Ad-hoc Committees

A. The Master's Board can establish committees or task forces for specific assignments that fall outside the direct scope or capacity of the joint governing bodies.

6. Set of Quality Assurance Procedural Documents

In the following section, the procedures and methodologies for quality enhancement are described into detail. For each procedure the objective is specified together with the data collection system, the data analysis system, and the enhancement system for suggesting and implementing improvements to the master's programme, as well as the available instruments for the procedure. References to the instruments are systematically coded for easy retrieval. For instance, IQH.03 refers to procedure 3 in the Internal Quality Handbook (i.e. the Procedure for Class Representative Meetings).

The specific actions detailed in the data collection system, the data analysis system and the enhancement system are to be implemented in a coordinated manner by the different Digital4Security partner institutions in their respective areas of competence. The different procedures explained into detail in this document are:

- IQH.01 Procedure for Academic Performance Analysis
- IQH.02 Procedure for Student Module Satisfaction Survey
- IQH.03 Procedure for Survey-Based Complementary Quality Management
- IQH.04 Procedure for Class Representative Meetings
- IQH.05 Procedure for Suggestions and Complaints
- IQH.06 Procedure for Quality Enhancement Planning

The outputs from Quality Assurance procedures are incorporated into an Annual Programme Review Report.

6.1. IQH.01 Procedure for Academic Performance Analysis

Internal Quality Procedure Reference	IQH.01
Title	Procedure for Academic Performance Analysis
Data Collection System	Each September, the Digital4Security Secretariat generates reports from the central administration system to assess cohort indicators for both Full-Time and Part-Time programmes. These include data such as (i) students who began each programme instance, (ii) current enrollment status in each programme, (iii) enrollment numbers for each module within both programmes.
Data Analysis System	The Project Coordinator and the QECD Committee analyze the academic performance indicators, diagnose possible causes for deviations from reference values and send an analysis report and improvement recommendations to the Master's Board of Directors in November.
Enhancement System	In November, the Master's Board of Directors considers the recommendations and delegates implementation of the enhancement measures to the Project Coordinator or specific partner institutions, unless decided otherwise.

6.2. IQH.02 Procedure for Student Module Satisfaction Survey

Internal Quality Procedure Reference	IQH.02
Title	Procedure for Student Module Satisfaction Survey

Data Collection System	Each term, the Secretariat distributes online surveys to student cohorts to gather feedback on their enrolled modules. Surveys are typically conducted in the second half of the teaching term, but before final exams. The module satisfaction survey covers subjects like course content, structure, workload relative to ECTS credits, practical applications, communication effectiveness, and inclusivity. Students have two weeks to complete the survey. The Secretariat processes survey responses within three weeks, supported by the QECD Committee. Results are compiled separately across the Full Time and Part Time programmes. They are summarized in a report shared with the Project Coordinator and Joint Programme Committee. Lecturers receive feedback on the modules they taught within two weeks of survey completion.
Data Analysis System	Annually, the QECD Committee monitors programme performance and prepares an Annual Programme Review Report summarizing key data, findings, and recommendations. This report is reviewed by the Master's Board of Directors, which may identify strategic adjustments. Lecturers review feedback on their modules to identify potential areas for improvement per teaching term.
Enhancement System	Based on the Annual Report, the Master's Board of Directors determines and delegates improvement measures to the Project Coordinators, QECD Committee, or partner institutions as needed. Lecturers use module-level feedback to explore alternative pedagogical strategies, if applicable, to enhance module delivery.

6.3. IQH.03 Procedure for Academic Performance Analysis

Internal Quality Procedure Reference	IQH.03
Title	Procedure for Survey-Based Complementary Quality Management
Data Collection System	The Secretariat distributes online surveys to various stakeholders to gather feedback. These typically include the following and can be selected

	based on guidance by the Master's Board of Directors in line with strategic objectives. ***(I) Student Feedback:*** In addition to the Module Satisfaction Survey (IQH.02), students are invited to provide feedback on their online learning experience, typically once during their first year and again in their final year of study. Feedback sections include the overall online study platform, navigation and usability, as well as the online learning experience. ***(II) Lecturer Feedback:*** After each module, or based on demand determined by the Master's Board of Directors, lecturers can be invited to provide feedback covering general module reflections, online teaching modality, student involvement and inclusivity, learning materials and tools, balance of practical vs. theoretical content, interaction and support, as well as feedback on the assessment process and grading. Additional feedback can be gathered on the appropriateness of assessment tasks for master's level, alignment with program learning outcomes, as well as the objectivity, reliability, and validity of grading, next to the completeness of topic coverage comparing the module content with assessment tasks. ***(III) Industry Expert Feedback:*** The industry expert survey is conducted regularly, such as once annually, aiming to collect at least two independent reviews per module, focusing on relevance to industry needs, content quality, inclusion of current issues and technologies, practical applications, and overall module assessments. Survey recipients have two weeks to complete the questionnaires.
Data Analysis System	The Secretariat processes survey responses within three weeks, supported by the QECD Committee. Performance is assessed, and findings are summarized in the Annual Programme Review Report, suggesting potential improvement measures. The Master's Board of Directors reviews this report to identify strategic adjustments and coordinates implementation with relevant bodies.
Enhancement System	The Master's Board of Directors decides on improvement strategies based on summary results from surveys as well as recommendations in the Annual Programme Review Report by the QECD Committee, delegating the implementation of improvement measures to the Programme and Project Coordinators, the QECD Committee and/or specific partner institutions, unless decided otherwise.

6.4. IQH.04 Procedure for Class Representative Meetings

Internal Quality Procedure Reference	IQH.04

Title	Procedure for Class Representative Meetings
Data Collection System	For each programme instance, during programme orientation, each cohort of students elect up to two individuals to act as class representatives. The role of the class representative is to act as a formal interface between cohorts of students and the teaching and administrative staff for issues that may potentially have an impact at the group level. The Master Secretariat establishes communication channels with the class representatives for each cohort at the beginning of each semester. In the sixth week of each semester, class representatives are requested to submit documented feedback on various aspects of their program, such as academic content, student services, timetabling, and any concerns or positive points they wish to raise. We then inform the representatives that a meeting is scheduled for the eighth week, where they, along with the Master's Board of Directors and the Project Coordinator, will discuss this feedback and address any arising issues. In the virtual environment, class representatives are elected via an online voting platform. Nominations are collected through the learning platform or email, and students vote anonymously in a secure online poll during the orientation period.
Data Analysis System	On receipt of the class representative feedback for each cohort, the Master Secretariat forwards the feedback documentation to the Master's Board of Directors and the Project Coordinator. A meeting is then scheduled (for week 8) with the class representatives, the Master's Board of Directors, and the Project Coordinator. The Master's Board of Directors and the Project Coordinator consider the feedback provided by the class representatives. A set of responses is compiled addressing any issues raised for discussion at the scheduled week 8 meeting.
Enhancement System	The Master's Board of Directors, and the Project Coordinator discuss any issues raised by the class representatives at the scheduled week 8 meeting. Potential improvement proposals are also discussed, and a set of actions and tasks are compiled as an output of the meeting. These actions and tasks are the responsibility of the Project Coordinator who then delegates completion of the tasks to the appropriate person(s) or groups.

6.5. IQH.05 Procedure for Suggestions and Complaints

Internal Quality Procedure Reference	IQH.04
Title	Procedure for Suggestions and Complaints
Data Collection System	Students wishing to suggest or comment about the programme policies or services, either academic or non-academic, can do so informally: • at the university by contacting the person in charge (where it seems appropriate), • by raising non-individual matters with the student class representatives • by raising individual matters with their student advisor or tutor. If informal channels do not suffice, formal suggestions and complaints can be submitted: • by sending a message to either a representative of the Master Secretariat or the Project Coordinator, • by writing a formal letter to the relevant Programme Director and/or joint Programme Coordinator, or if the complaint is lodged against the Programme Director and/or Joint Programme Coordinator, by writing to the President of the Project Coordinator's institution.
Data Analysis System	The addressee of a complaint will keep the name of the issuer or any other reference anonymous (unless the complainer states otherwise) and facilitate a prompt resolution of the complaint. • The Master's Board will consider complaints about academic judgments, and about matters to do with the student's course of study or research, only if the candidate is not satisfied with the outcome reached by the partner institution associated with the module for which there is a complaint. • Regarding results of examinations the Board may function as a Review Committee only if the student is not satisfied with the outcome reached at the partner institution via interaction with the relevant Programme Coordinator. • Concerning the handling of complaints of academic judgments and the effective organization of tests and examinations the partner institutions guarantee a system that adequately takes into account the specific nature of the joint programme and its exigencies.
Enhancement System	An initial response to any complaint can be expected within 7 days of complaint receipt, and a considered response to the complaint should be

	received within a further three weeks, with any subsequent remedy implemented with the minimum of delay.

6.6. IQH.06 Procedure for Quality Enhancement Planning

Internal Quality Procedure Reference	IQH.05
Title	Procedure for Quality Enhancement Planning
Data Collection System	The QECD Committee decides on the organization of improvement actions that have been delegated to it by the Master's Board of Directors. The QECD Committee ensures that for every (major) improvement action a person is appointed as responsible for monitoring the improvement action during implementation and at completion. On completion, the appointed person creates an evaluation report which is made available to the Programme Coordinator, the QECD Committee and the Joint Programme Committee.
Data Analysis System	In cooperation with the Programme Coordinator, the QECD Committee compiles an overview report based on the improvement action evaluation reports. This is sent accompanied with recommendations for further action to the Board of Directors. These recommendations may include concrete proposals for modifications of the Internal Quality Handbook itself.
Enhancement System	The Master's Board of Directors adopts the recommendations and proposals and delegates their implementation to the Programme Coordinator, the QECD Committee and/or partner institutions involved, unless decided otherwise.

Project 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03

Digital4Security

Shaping Europe's cyber future

ADVANCED DIGITAL SKILLS

DIGITAL EUROPE PROGRAMME

Co-funded by the European Union

Student Handbook

Digital4Security

Shaping Europe's cyber future

Project details: Joint Master's Degree Programme
in Cybersecurity Management & Data Sovereignty (Digital4Security)

Project ID: 101123430

Call: DIGITAL-2022-SKILLS-03

Table of Contents

Welcome to Your Programme

Welcome to the Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty programme. This is a highly innovative, effective, and sustainable European postgraduate degree programme offered by a consortium of Higher Education Institutes and developed via an industry-led approach in conjunction with D4S industry partners. The programme covers essential areas such as AI, data science, cybersecurity, and cloud technologies. In particular, the programme focuses on meeting the needs for advanced digital skills within European SMEs and companies across a range of industry sectors, helping businesses achieve long-term competitiveness and growth through digital transformation and innovation. These skills are pivotal to European businesses' ongoing competitiveness and growth.

The purpose of this handbook is to provide you with key information as to how the programme is delivered, its structure, how you will be assessed, student services that you can avail of, and relevant policies and procedures. The information in this handbook outlines what you can expect at each stage of your studies.

We hope you find this programme of study interesting, enjoyable, and rewarding.

The Digital4Security Project

Digital4Security is a ground-breaking pan-European master's program aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. This €20m industry-led Master's, supported by funding from the DIGITAL Europe Programme, is a four-year initiative that comprises a Consortium of 36 partners spanning 12 countries. This master program will provide comprehensive knowledge of cybersecurity management, regulatory compliance, and technical expertise to European SMEs and companies.

Digital4Security is launching a collective cybersecurity revolution by harnessing the collective skill sets of our international Consortium, and the next generation of practical experts in the digital space. We're reskilling and upskilling graduates, professionals, managers and business leaders to become 'cyber confident', equipped to protect and empower European SMEs in the face of global cyber threats.

The Digital4Security curriculum is grounded in a rigorous needs analysis process involving all of our Consortium partners. The programme will blend academic and industry content to ensure graduates are equipped with both theoretical and job-ready cyber skills to fast-track employment. The program is designed to meet European accreditation standards and a wide range of national standards, with plans to offer micro-credentials for each module and industry certification in collaboration with our industry partners.

D4S Consortium

The Digital4Security Consortium is a dynamic pan-European partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management programme, developed and delivered by the best cybersecurity talent from Europe and worldwide. Table 1 lists the Higher Education Institutions (HEIs) jointly offering the master's degree, while Table 2 presents additional consortium partners, including industry stakeholders.

Table 1: Academic Partners (Higher Education Institutes) Offering the Joint Degree Program

No.	Partner	Abbreviation	Country
1	Universitatea Nationala de Stiinta si Technologies Politehnica Bucuresti	POLITEHNICA B.	Romania
2	National College of Ireland	NCI	Ireland
3	German University of Digital Science gGmbH	UDS	Germany
4	University of Rijeka	UNIRI	Croatia
5	Università degli Studi di Brescia	UNIBS	Italy
6	Politecnico di Milano	POLIMI	Italy
7	Universität Koblenz	UNI KO	Germany
8	CY Cergy Paris Université	CY	France
9	Mykolo Romerio Universitetas	MRU	Lithuania
10	Universidad Internacional de La Rioja	UNIR	Spain
11	Brno University of Technology	BUT	Czech Republic
12	Munster Technological University	MTU	Ireland
13	Vytautas Magnus University	VMU	Lithuania

Table 2: Associate Partners

No.	Associated Partner	Abbreviation	Country
14	DIGITAL TECHNOLOGY SKILLS LIMITED	DTSL	Ireland
15	IT@CORK ASSOCIATION LIMITED LBG	IT@CORK	Ireland
16	SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	SKILLNET	Ireland
17	ADECCO FORMAZIONE SRL	ADECCO TRAINING	Italy
18	ADECCO ITALIA HOLDING DI PARTECIPAZIONE E SERVIZI SPA	ADECCO GROUP	Italy
19	ADECCO ITALIA SPA	Adecco Italia	Italy
20	CEFRIEL SOCIETA CONSORTILE A RESPONSABILITA LIMITATA SOCIETA BENEFIT	CEFRIEL	Italy
21	ATAYA & PARTNERS	Ataya	Belgium
22	CYBER RANGES LTD	Cyber Ranges	Cyprus
23	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	FHG	Germany
24	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	NASK	Poland
25	POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	CMIP	Poland
26	SCHUMAN ASSOCIATES SCRL	SA	Belgium
27	CONTRADER SRL	Contrader	Italy
28	INDEPENDENT PICTURES LIMITED	indiepics	Ireland
29	MATRIX INTERNET APPLICATIONS LIMITED	MATRIX	Ireland
30	PROFIL KLETT D.O.O.	PROFIL KLETT	Croatia
31	SERVICENOW IRELAND LIMITED	ServiceNow	Ireland
32	EUROPEAN DIGITAL SME ALLIANCE	DIGITAL SME	Belgium
33	DIGITALEUROPE AISBL*	DIGITALEUROPE	Belgium
34	TERAWE TECHNOLOGIES LIMITED	TERAWE	Ireland
35	BANCO SANTANDER SA	BANCO SANTANDER /Santander	Spain
36	RED OPEN S.R.L.	RED OPEN S.R.L.	Italy

The HEIs, in conjunction with the Digital4Security consortium's industry partners, have collaborated and cooperated to jointly develop and design this programme and its curriculum.

The Digital4Security Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty

This Master's programme is delivered online and it composed of 120 ECTS organized in 23 modules: 9 mandatory modules and a set of 14 elective modules to complete for training according to your interest.

All these modules are intended to help you to achieve the following set of learning outcomes in Table 3, developed to align with industry feedback and the analysis of related programmes internationally:

Table 3: Overarching Learning Goals across the Joint Degree Program

No.	Goal
PO1	Critically assess and evaluate cybersecurity principles, practices, and technologies relevant to modern enterprises.
PO2	Strategically apply cybersecurity knowledge and utilise practical skills and technologies for long-term success in cybersecurity leadership roles across diverse industries, government agencies, and institutional settings.
PO3	Identify knowledge gaps and undertake self-learning to acquire new knowledge to support professional development and the ability to adapt to evolving threats, technologies, and regulatory environments.
PO4	Exhibit and apply leadership skills necessary for effectively managing cybersecurity initiatives within organisations, including education and training, strategic planning, and resource allocation.
PO5	Critically evaluate and analyse cyber threats in order to implement effective security operations, and to enable the proactive identification, assessment, and mitigation of cyber threats.
PO6	Effectively apply analytical and strategic thinking in order to make decisions to address security requirements.
PO7	Communicate effectively across a range of complex and advanced cybersecurity concepts to provide leadership within an organisation and facilitate effective collaboration and teamwork.
PO8	Critically assess cybersecurity legal, information governance, and regulatory frameworks and practices to ensure effective oversight, auditing, risk mitigation, accountability, compliance, and strategic alignment with organisational objectives.

Programme Structure and Delivery Modes

The Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty is delivered fully online using a combination of synchronous and asynchronous delivery techniques. Therefore, there is no requirement for learners to physically attend classes at any partner institution's geographical location.

The fully online delivery of the programme is facilitated by utilising a centralised Learning Management System (LMS) and virtual classroom technologies.

The programme is offered in two modes of study:

i) Full Time,
ii) Part Time.

Table 4 provides information of the expected period of study for each of these delivery schedules.

Table 4. Duration of the Programme for each Mode of Study

Name	Mode of study	Intake rhythm	Average time required to complete studies
Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty	Full time	Each semester	4 semesters / 2 years
	Part time	Each semester	6 semesters / 3 years

Note: A semester is an academic session that typically encompasses 12 weeks of teaching and a further period of time to allow for module terminal examinations after the 12th week.

Study load for the programme is expressed in credits of the European Credit Transfer and Accumulation System (ECTS). composed of 120 ECTS.

For a learner registered on the Full-Time programme, the standard period of study is two years. The programme schedule and the curriculum are designed in a way that allows students to earn 30 ECTS per semester over four semesters. The workload per semester consists of an average 750 hours.

For a learner registered on the Part Time programme, the standard period of study is three years. In this case, the programme schedule and the curriculum are designed in a way that allows students to earn 20 ECTS per semester over six semesters.

To the greatest extent possible, the programme schedule is designed to distribute the workload evenly across the semester by offering a variety of teaching and assessment formats.

Full Time Delivery

The Figures 1 to 8 provide tailored programme structures for the Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty (Full Time).

Fig. 1: A 120 ECTS Master's Program Preparing for the Role of *Chief Information Security Officer (CISO)* - Possible Pathway in a 2-Year Full Time Program

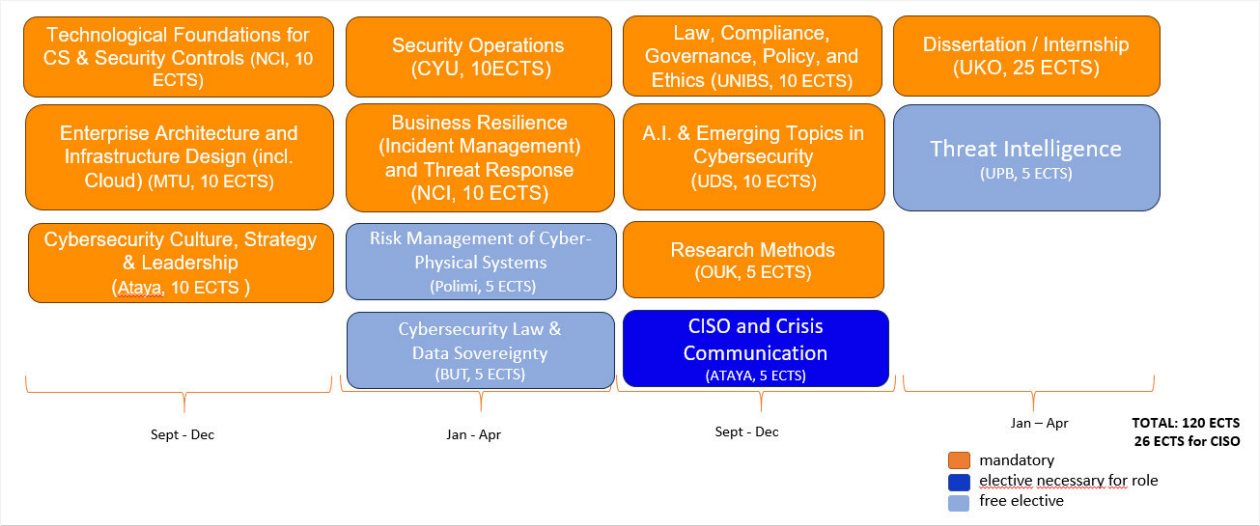


Fig. 2: A 120 ECTS Master's Program Preparing for the Role of *Cyber Legal, Policy, and Compliance Officer* - Possible Pathway in a 2-Year Full Time Program

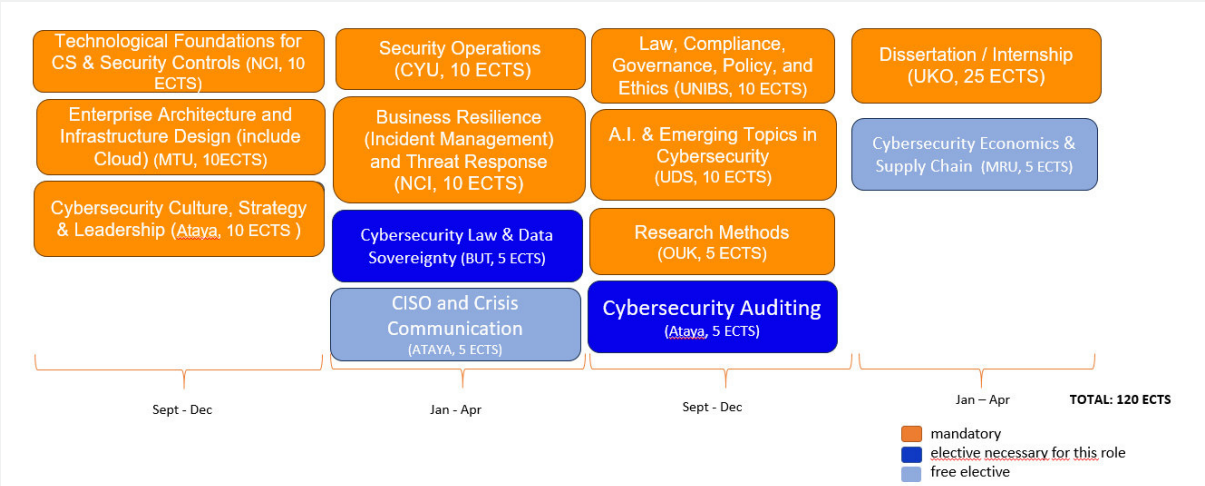


Fig. 3: A 120 ECTS Master's Program Preparing for the Role of *Cybersecurity Risk Manager* - Possible Pathway in a 2-Year Full Time Program

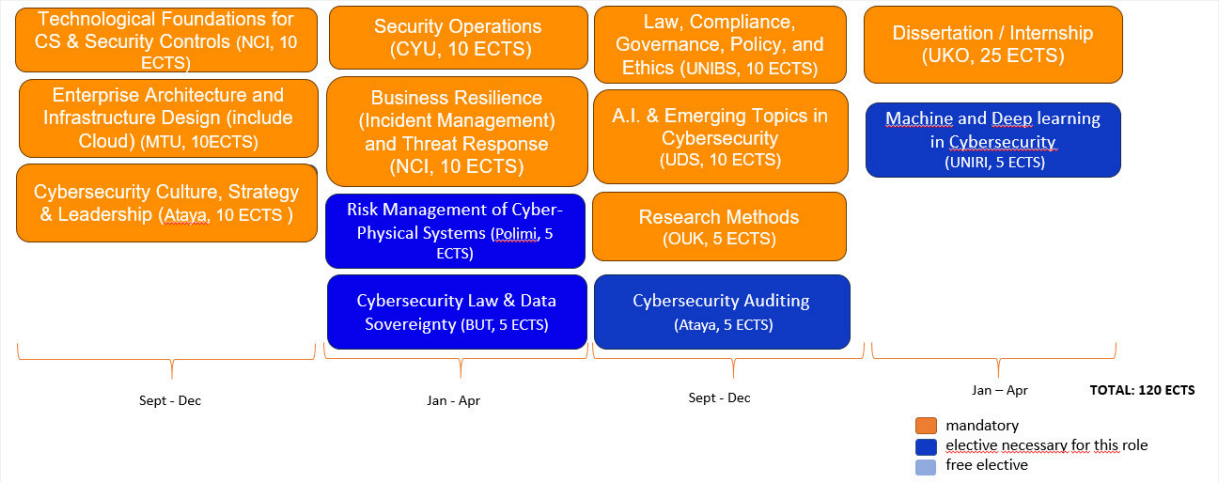


Fig. 4: A 120 ECTS Master's Program Preparing for the Role of *Cyber Threat Intelligence Specialist* - Possible Pathway in a 2-Year Full Time Program

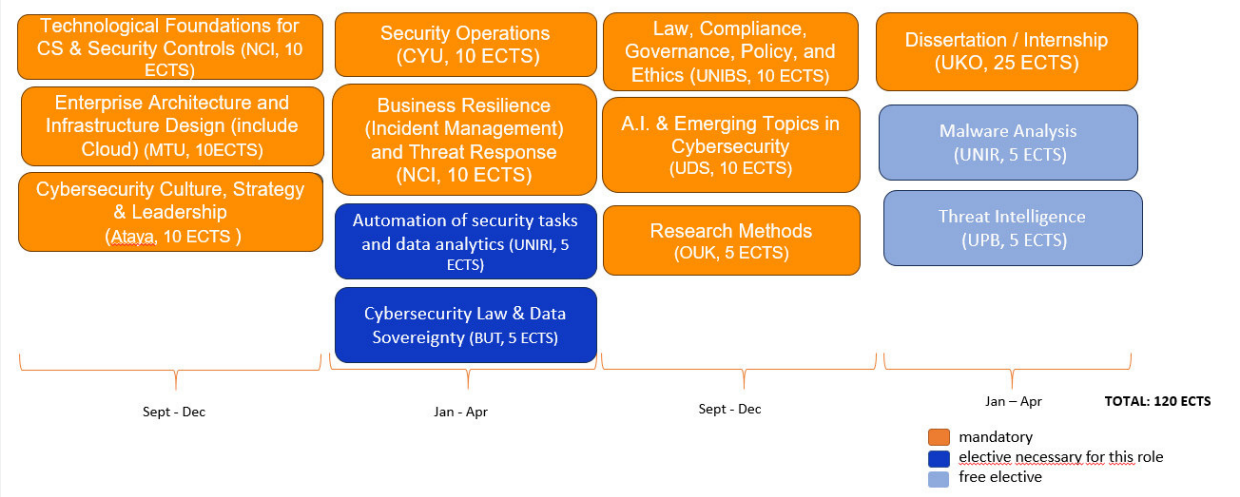


Fig. 5: A 120 ECTS Master's Program Preparing for the Role of *Cybersecurity Educator* - Possible Pathway in a 2-Year Full Time Program

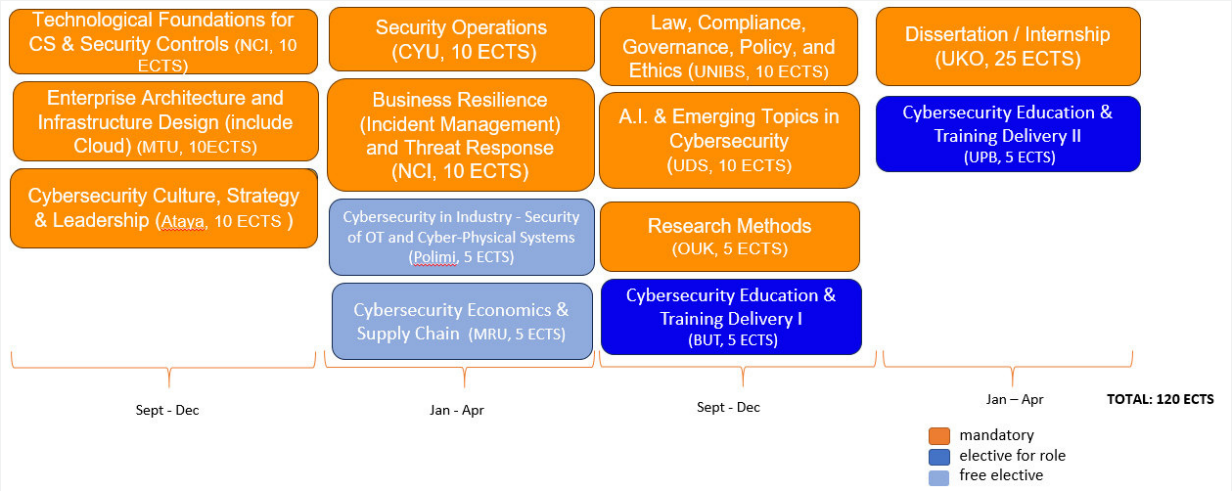


Fig.6: A 120 ECTS Master's Program Preparing for the Role of *Cybersecurity Auditor* - Possible Pathway in a 2-Year Full Time Program

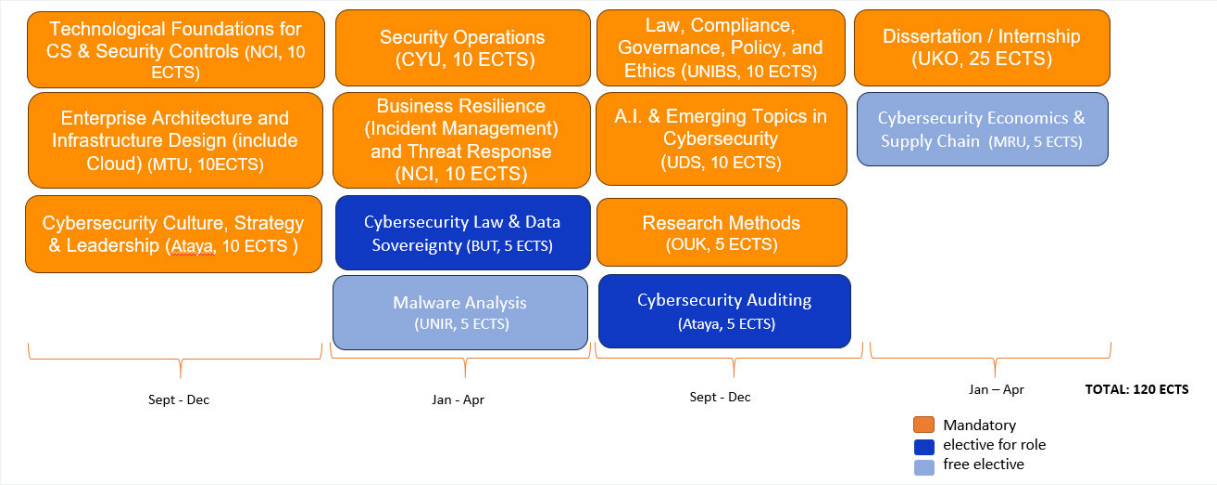


Fig. 7: A 120 ECTS Master's Program Preparing for the Role of *Digital Forensics Investigator* - Possible Pathway in a 2-Year Full Time Program

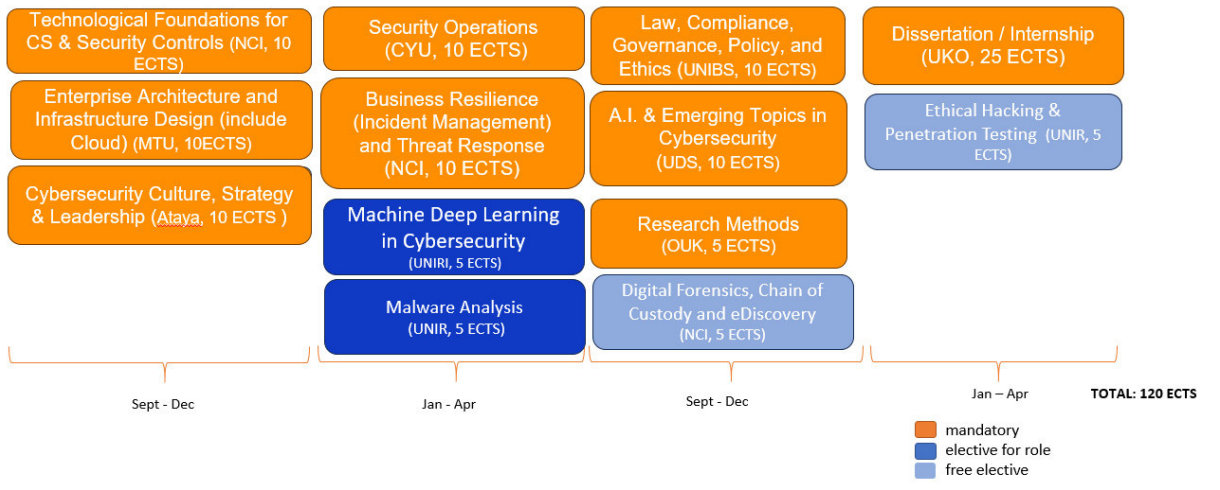
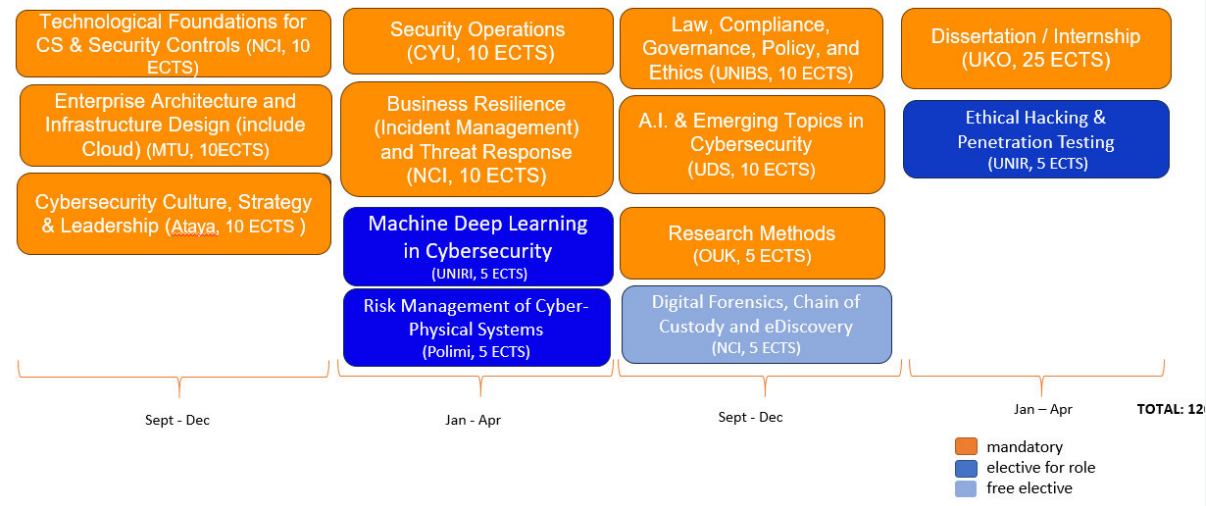


Fig. 8: A 120 ECTS Master's Program Preparing for the Role of *Incident Responder* - Possible Pathway in a 2-Year Full Time Program



Choice of Elective Modules

There is a high degree of flexibility for learners when choosing elective modules (cf. Table 5). The programme team's analysis of role profiles offer guidance to learners with regards to which elective modules are a more suitable choice to make when pursuing such roles.

Note: the elective modules that are offered for learners to choose from in any given semester may be restricted due to operational scheduling constraints and/or the overall learner demand for

choosing particular elective modules. Notwithstanding this, the programme team will endeavour to accommodate the broadest offering of elective modules each semester under these constraints.

Table 5. Module ECTS, Mandatory/Elective Status, and Corresponding Partner Institute

NO.	SUBJECT	ECTS	MAND/ELECT	PARTNER
1	AI & Emerging Topics in Cybersecurity	10	Mandatory	UDS
2	Business Resilience, Incident Management, and Threat Response	10	Mandatory	NCI
3	Cybersecurity Culture, Strategy & Leadership	5	Mandatory	VMU
4	Dissertation / Internship	25	Mandatory	UNI KO
5	Enterprise Architecture, Infrastructure Design and Cloud Computing	10	Mandatory	MTU
6	Law, Compliance, Governance, Policy, and Ethics	10	Mandatory	UNIBS
7	Research Methods	5	Mandatory	UNI KO
8	Security Operations	10	Mandatory	CY CERGY
9	Technological Foundations for CS & Security Controls	10	Mandatory	UPB
10	Automation of Security Tasks and data analytics	5	Elective	UNIRI
11	CISO and Crisis Communication	5	Elective	VMU
12	Risk Management of Cyberphysical Systems	5	Elective	POLIMI/ CEFRIEL
13	Cybersecurity Auditing	5	Elective	VMU
14	Cybersecurity Economics & Supply Chain	5	Elective	MRU
15	Cybersecurity Education & Training Delivery I	5	Elective	BUT

16	Cybersecurity Education & Training Delivery II	5	Elective	UPB
17	Cybersecurity in Industry - Security of OT and Cyber-Physical Systems	5	Elective	POLIMI
18	Cybersecurity Law & Data Sovereignty	5	Elective	BUT
19	Machine and Deep Learning in Cybersecurity	5	Elective	UNIRI
20	Digital Forensics, Chain of Custody and eDiscovery	5	Elective	NCI
21	Ethical Hacking & Penetration Testing	5	Elective	UNIR
22	Malware Analysis	5	Elective	UNIR
23	Threat Intelligence	5	Elective	UPB

Language of Instruction

The programme is delivered using English as the language of instruction.

Summary Description of Programme Modules

Table 6 provides a summary description and a set of learning outcomes for each of the programme's modules.

Note: Further detailed information for each module is avaiable in the Module Descriptor Handbook document.

Table 6. Module Summary Overview and Learning Objectives

Module Title	Mandatory / Elective	ECTS	Module Overview	Module Learning Objectives
AI & Emerging Topics in Cybersecurity	M	10	The module delves into AI and its impact on cybersecurity, highlighting its offensive and defensive applications. Using both lectures and flipped classroom sessions, students will learn key AI concepts and their applications in today's Security Operations Centers (SOCs). Finally, they will apply their learning in a group project, developing AI-powered cyber defense or attack scenarios.	PO1 PO2 PO3 PO5 PO6 PO8
Business Resilience, Incident Management, and Threat Response	M	10	This module aims to provide learners with knowledge on documentation, strategies, and technologies that support the processes of business resilience, threat response, and incident management. The module will examine how an organisation can prepare for business disruption and what actions can be taken to prevent and contain an incident, reduce the impact to organisational systems and get the business operational as quickly as possible after an incident occurs. Learners will acquire the necessary incident management skills required to develop contextual plans, run books and the associated processes and tools to enable effective business resilience capabilities. Furthermore, learners will be able to identify and illustrate the challenges associated with developing risk-based business resilience, threat response, and incident management processes. Learners will gain practical experience in aligning an organisation to industry standards and best practices that are commonly used for business resilience, threat response, and incident management tasks incorporating several stages,	PO1 PO2 PO3 PO4 PO5 PO6 PO7 PO8

			including preparation for incidents, detection and analysis of a security incident, containment, eradication, and full recovery, and post-incident analysis and learning.	
Cybersecurity Culture, Strategy & Leadership	M	5	Management practices for Chief Information Security officers and those reporting to this function include various management practices, involve specific culture and involves developing adequate strategy. This module addresses those management practices and train students on understanding and applying those practices. It includes implementing those processes and practices including the seven maturity components to ensure resilient operations.	PO1 PO2 PO3 PO4 PO5 PO6 PO8
Dissertation / Internship	M	25	Dissertation: After taking this module, you will have knowledge of research in your specialisation area. You will have an understanding of academic theory and the preparation of research pertinent to your field of study. You will be able to select appropriate research methods and techniques suitable for your research field You will understand the current state of the art in your research area, and be able to appropriately employ methods and existing research results in the development of new knowledge, theories and presentation of research in your research area Internship: After taking this module, you will be able to analyse employer requirements and be able to articulate one's skills and experience related to these. You will be able to effectively demonstrate one's professional skills in a work environment. You will be able to critically reflect on the learning activities and experiences from the internship.	Dissertation: PO1 PO2 PO3 PO6 PO7 Internship: PO3 PO4 PO6 PO7

			You will be able to create an individual learning plan to identify meaningful personal and professional goals.	
Enterprise Architecture, Infrastructure Design and Cloud Computing	M	10	Evaluate the importance of enterprise security architecture and infrastructure design to protect the organisation's systems and data from cybersecurity and other digital threats. Appraise the key computer network controls required to protect a network from various forms of attack. Analyse the security of cloud environments, identifying the critical similarities and differences between cloud and network security.	PO1 PO2 PO5 PO6
Law, Compliance, Governance, Policy, and Ethics	M	10	The "Law, Compliance, Governance, Policy, and Ethics" module focuses on equipping students with an in-depth understanding of the legal, ethical, and governance frameworks that shape cybersecurity practices. It provides comprehensive insights into data protection laws, governance structures, and the intersection of legal and ethical standards in organizational cybersecurity strategies. Students will engage with real-world applications of laws such as the GDPR, NIS2, and the Cyber Resilience Act learning how to implement compliance measures and ethical practices in diverse cybersecurity environments. Through case studies, discussions, and practical exercises, students will develop the skills needed to craft and assess policies, promote ethical cybersecurity practices, and lead with integrity in professional settings.	PO1 PO2 PO4 PO6 PO8
Research Methods	M	5	After taking this module, you will be able to fully understand the range of research approaches, methodologies and strategies used in research within Cyber Security. You will have the tools and knowledge by which you can design a research proposal in Cyber Security applying relevant research strategies to collect and test data.	PO1 PO2 PO3 PO5 PO6 PO7

Security Operations	M	10	The "Law, Compliance, Governance, Policy, and Ethics" module focuses on equipping students with an in-depth understanding of the legal, ethical, and governance frameworks that shape cybersecurity practices. It provides comprehensive insights into data protection laws, governance structures, and the intersection of legal and ethical standards in organizational cybersecurity strategies. Students will engage with real-world applications of laws such as the GDPR, NIS2, and the Cyber Resilience Act learning how to implement compliance measures and ethical practices in diverse cybersecurity environments. Through case studies, discussions, and practical exercises, students will develop the skills needed to craft and assess policies, promote ethical cybersecurity practices, and lead with integrity in professional settings.	PO1 PO2 PO5 PO6
Technological Foundations for CS & Security Controls	M	10	The “Technological Foundations in Computer Science and Security Controls” aims to create the fundamental set of skills and knowledge in computing systems and security. Students will gain understanding and competences expected for a system power user: investigate, update, configure, assess, monitor a computing system and its components, with particular focus on security.	PO1 PO2 PO5 PO6
Automation of Security Tasks and data analytics	E	5	This course provides a comprehensive introduction to using Python for automating cybersecurity tasks, including threat detection, intelligence gathering, vulnerability assessment, and incident response. Students will learn to write scripts, analyze data and integrate various tools, while adhering to ethical and legal guidelines in cybersecurity automation.	PO1 PO2 PO5 PO6 PO8

CISO and Crisis Communication	E	5	Cybersecurity Communication activities are essential in crisis situations and as regular communication of the CISO to stakeholders. Crisis communication is required for three specific focuses that are: Communicate to resolve the incident and the crisis; Communicate as a compliance notification required by law and regulators; and finally communicate to improve the reputation as a follow-up on an incident/crisis. Mastering communication activities is a must skill for cybersecurity leaders.	PO1 PO2 PO4 PO5 PO6 PO7 PO8
Risk Management of Cyberphysical Systems	E	5	The Risk Management of Cyber-Physical Systems module aims to equip students with the skills to analyse, assess, and manage risks associated with socio-cyber-physical systems. It provides a comprehensive understanding of complexities and practices in technology risk governance (in the different stages of the system life cycle), and in operational resilience, through practical applications of industry-recognized methods, tools and processes. Students will analyse case studies and engage with a serious game to gain practical insights into the interplay between cybersecurity and business continuity. The module includes three core instructors and features guest lectures from industry professionals, offering valuable practitioner perspectives.	PO1 PO2 PO5 PO6
Cybersecurity Auditing	E	5	The Cybersecurity Economics & Supply Chain module aims to equip students with comprehensive knowledge of the economic aspects of information security and supply chain cybersecurity. It covers key concepts such as the direct and indirect costs of cyber incidents, the economic impact of various cyber threats on organizations, and the strategic role of cybersecurity in business planning. Students will explore frameworks, budget allocation for cybersecurity, and methods for managing third-party risks in supply chains. Through interactive lectures, practical exercises, and case studies,	PO1 PO2 PO4 PO6 PO7 PO8

			students will learn to conduct qualified investment analyses, understand technical incident reports, and apply economic models in security. Graduates will be able to strategically plan cybersecurity processes and evaluate the economic efficiency of security solutions within organizations and supply chains.	
Cybersecurity Economics & Supply Chain	E	5	The Cybersecurity Economics & Supply Chain module aims to equip students with comprehensive knowledge of the economic aspects of information security and supply chain cybersecurity. It covers key concepts such as the direct and indirect costs of cyber incidents, the economic impact of various cyber threats on organizations, and the strategic role of cybersecurity in business planning. Students will explore frameworks, budget allocation for cybersecurity, and methods for managing third-party risks in supply chains. Through interactive lectures, practical exercises, and case studies, students will learn to conduct qualified investment analyses, understand technical incident reports, and apply economic models in security. Graduates will be able to strategically plan cybersecurity processes and evaluate the economic efficiency of security solutions within organizations and supply chains	PO1 PO2 PO3 PO4 PO5 PO6 PO8
Cybersecurity Education & Training Delivery I	E	5	3-4 sentences summarizing the objectives, content and methods. Something along the lines: "The Cybersecurity Education and Training Delivery module aims to prepare students to identify weaknesses, raise awareness and develop training programs in the realm of cybersecurity education. It presents an array of technical tools and modern methodology to teach cybersecurity related content while combining it with fundamental pedagogical principles. Students will be able to plan and carry out cybersecurity trainings, which will further be developed in the second module of this kind.	PO1 PO2 PO4 PO6 PO7

Cybersecurity Education & Training Delivery II	E	5	The "Cybsersecurity Education and Training Delivery II" module aims to build the required skills for students to be creators of practical cybsersecurity contests and use competition-based learning in their educator role. Students will learn how to design, implement, deploy and grade challenges as part of cybsersecurity contests (e.g. CTF – Capture the Flag). These are to be used as part of training and teaching activities that students will conduct themselves.	PO1 PO2 PO4 PO5 PO6 PO7
Cybersecurity in Industry - Security of OT and Cyber-Physical Systems	E	5	This module aims to equip learners with comprehensive knowledge and practical skills in OT (Operational Technology) security, highlighting the differences and overlaps with IT (Information Technology) security. The focus will be on understanding key principles, risk modelling, and the legal and regulatory landscape, alongside developing skills to analyse, evaluate, and implement effective security measures in industrial environments.	PO1 PO2 PO5 PO6 PO7 PO8
Cybersecurity Law & Data Sovereignty	E	5	Cybersecurity and Cybercrime The content of this part of the module will cover the main concepts and structure of the cybersecurity law and criminal law applicable to cybercrime. The first area will include the theory and practice of cybersecurity obligations based on category of the regulated subject; liability for cybersecurity incidents; relevant case law; and tools for coordination and standardisation of cybersecurity compliance, such as cybersecurity certification. In the second area, we will cover relevant legal provisions of substantive and procedural criminal law; categorisation of cybercrimes; as well as European and international procedural tools used in investigation and prosecution of cybercrime. Data Sovereignty This part of the module is aimed at an in-depth exploration of the legal dimensions of specific	PO1 PO3 PO4 PO6 PO8

			aspects of data sovereignty and specific regimes applicable under the EU law. It prepares students to navigate the complex legal landscape in specific areas connected to various forms of data flows, in order to be able to ensure compliance in their professional practices within the EU. Apart from the regulatory regimes for processing personal data, participating in data spaces or doing business through online platforms, the content will include rules and requirements applicable to handling of electronic documents, including the relevance for constituting electronic evidence, and to the use of electronic identification and digital identity in particular in its application in the public law processes.	
Machine and Deep Learning in Cybersecurity	E	5	This module focuses on applying machine learning and deep learning techniques to cybersecurity challenges such as anomaly and malware detection, fraud detection, and spam classification. Students will explore various machine learning algorithms, analyze their performance, and design appropriate models for specific cybersecurity tasks. The course also covers explainability issues in AI-driven cybersecurity, alongside hands-on labs using Python and popular libraries like Scikit-learn, TensorFlow, and PyTorch.	PO1 PO2 PO5 PO6
Digital Forensics, Chain of Custody and eDiscovery	E	5	This module aims to enable learners to develop a knowledge, skills and competence to approach a Digital Forensics investigation whilst safe-guarding the chain of custody of acquired digital forensic evidence. This module also aims to develop skills associated with eDiscovery. Learners will gain practical experience in using various tools used in Windows forensics, Linux forensics, mobile forensics, network forensics and eDiscovery. This module provides an in-depth coverage of various sub-domains of digital forensics and how it is related to eDiscovery.	PO1 PO2 PO5 PO6 PO7 PO8
Ethical Hacking & Penetration Testing	E	5	This module will allow the student to understand, analyze and manage the ethical hacking process by learning the concepts, techniques and processes through videos, practical exercises and laboratories. Obtaining the ability to use the	PO1 PO2 PO5

			results of an audit for management and decision making.	PO6
Malware Analysis	E	5	This module will allow the student to understand, analyze and manage the malware analysis process by learning the methods, techniques and tools used. With exercises, videos and laboratories the student will learn the importance and how to use the results for auditing and other cybersecurity processes.	PO1 PO2 PO5 PO6
Threat Intelligence	E	5	This module aims to introduce the fundamentals of Cyber Threat Intelligence (CTI). The lectures will present the CTI lifecycle, highlight strategic integration and discuss emerging trends in this field. The students will learn how to identify threat intelligence data streams, apply the extracted information for vulnerability assessment and threat mitigation, and disseminate newly acquired knowledge into public databases.	PO1 PO2 PO4 PO5 PO6 PO7 PO8

Digital4Security Master's Governance and Management Structure

The Master's degree programme has the following management structures defined with responsibilities of decision, of evaluation and execution:

Master's Board of Directors

The Master's Board of Directors is comprised of Programme Directors that have been selected by each of the Partner Institutions to represent them on all matters concerning the degree programme. The Master's Board is responsible for general management, academic supervision, quality assurance, degree awarding and recognition issues, agreement changes, dispute resolution and student complaints. Additionally, the Master's Board is responsible for the system review, advice on policy developments for the joint degree programme, and to ensure the coherence and consistency of the concept of the programme. The Master's Board meets

at least twice each year. Initial minutes of the Master's Board meeting are compiled by the Secretariat and distributed to all members of the Master's Board within fifteen days after the meeting. Any changes to the draft minutes must reach the Programme Secretariat within one week after the distribution of the minutes. After this deadline, the Programme Secretariat shall produce and file a final version, a copy of which shall also be sent to all Programme Directors.

The Programme Secretariat (including Programme Coordinators)

The Secretariat is responsible for the daily operation and administrative management of the programme guided and governed by the Master's Board. The Secretariat is partly based at the Project Coordinator Institution, also designated as the Master's Secretariat. The secretariat, supports the coordination and day-to-day management of the programme, its support mechanisms, specifically tasks regarding quality assurance, application, selection and student admission and administration, and mobility coordination. The Secretariat also includes a wider group of Programme Coordinators, from each of the partner institutions Partner Programme Coordinator representatives will liaise with Programme Coordinators from other partner institutions and provide administrative support to the Secretariat for issues arising that are associated with the partner institution they are representing. The Secretariat also provides direct support for the Master's Board Meetings (the minutes), the public website, and other tasks assigned by the Master's Board.

The Joint Admissions Board

Assisted by the Secretariat and under the supervision of the Master's Board, the Joint Admissions Board is responsible for the selection and admission of all students to the degree programme. The Joint Admissions Board shall consist of one representative from each Partner Institution. The Partner Institution is responsible for appointing its representative in accordance with its own procedures and national regulations. The Joint Admissions Board convenes at least once after each application deadline and can hold additional meetings until a selection and admission procedure is completed.

The Examinations Board

The Examinations Board is headed by the Master's Board of Directors. The Master's Board is responsible for the overall quality and standards of the degree programme and for agreeing the academic standards. It monitors the partner institutions' compliance and is responsible for the degree programme being delivered to the highest academic standards. The Examinations Board may be supplemented with additional nominees from Partner Institutions that have expertise in quality assurance and those who are responsible for programme examination administration. Meetings of the Examinations Board convene after each programme examination session and on completion of grading and the assessment of learners' exam scripts, project submissions, or other relevant coursework by programme faculty. The Examinations Board deliberates cases, brought to its attention in at least one week's notice. If the nature of the case brought to its attention demands a swift ruling, a special meeting may

be arranged or by written consultation of its members via electronically mediated systems. All assessments are conducted in accordance with the jointly agreed policies and procedures for the degree programme as adopted by the Master's Board (specifically in accordance with the Study and Examination Regulations).

The Joint Programme Committee

The Joint Programme Committee acts as advisor to the Master's Board of Directors. It is responsible for the system review and advice on policy developments for the joint degree programme. The Joint Programme Committee meets physically at least once a year to ensure the coherence and consistency of the concept of the joint degree programme. Additional meetings can be held as required. The Joint Programme Committee is composed of representatives from the Secretariat, Programme Coordinators, the Master's Board of Directors, Faculty representatives, and representatives from the Quality Enhancement and Curriculum Development Committee.

The Quality Enhancement and Curriculum Development (QECD) Committee

The Quality Enhancement and Curriculum Development Committee is composed of at least one academic faculty member from each Partner Institution. The QECD Committee prepares and implements on behalf of the Master's Board of Directors, quality enhancement and curriculum development. It strengthens the collaborative nature of the degree program by following the European Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG). The Quality Enhancement and Curriculum Development (QECD) Committee reports to the Master's Board. The QECD Committee meets whenever called upon or whenever the annual internal quality procedures as detailed in the Internal Quality Handbook of the Programme require, either in person or via electronically mediated systems.

The Quality Enhancement and Curriculum Development (QECD) Committee supports the Joint Programme Committee in assessing how well the program meets its learning objectives and maintains coherence. It also ensures effective processes are in place for data collection, analysis, making recommendations, and channelling suggestions to improve the programme.

The Project Coordinator

The Project Coordinator is responsible for:

- Student Recruitment, Onboarding, and Support: Managing recruitment, onboarding, and support processes, including the use of digital platforms and supplementary events.
- Industry Certifications & Micro-Credentials: Implementing industry certifications and micro-credentials.
- Employability Programme: Establishing an employability programme for students.

- European Mobility Programme: Facilitating student and lecturer mobility between institutions and companies.
- Faculty Training Resources: Providing resources for faculty training and support.

Moreover, the Project Coordinator has overall coordination responsibility for the degree programme. He/she represents the Digital4Security consortium partnership before the Commission and reports to the Master's Board and other stakeholders on the operation and programme coordination issues and quality enhancement outcomes.

Faculty Members

The programme's teaching staff includes academics from each of the partner institutions directly involved in the design, development, and delivery of the programme. It comprises highly qualified lecturers and researchers with a broad range of expertise across the spectrum of subjects associated with advanced digital skills. The primary responsibility of the program faculty is to develop curriculum ideas, create innovative teaching materials and methods, engage in professional discussions with fellow academics, and promote interdisciplinary thinking across different subjects They may participate in teacher exchange and joint teaching programme design. The programme faculty members focus on approaches to teaching and learning, assessment and performance, and comparative analysis of student workload. The faculty is committed to providing the best possible service to students of the Masters programme.

Teaching, Learning and Assessment on the Joint Master's Degree Programme

The Teaching, Learning and Assessment (TLA) strategy for the programme provides learners with an innovative mix of approaches to engage with the content of their modules and to demonstrate their learning. The TLA strategy seeks to combine lectures, tutorials, problem-based learning (PBL), enquiry-based learning, practical work, the flipped classroom, seminars, case-based learning, project-based work, and group work which are all recognised as effective teaching and learning methods.

Central to the strategy on this programme is the belief that the learner is an active participant in the learning process and not simply a passive recipient of information. Teaching on this programme therefore aims to make content relevant to the worlds of work and community and, aims to create opportunities for learners to interact with each other as well as with faculty from partner HEIs in a mutually supportive learning environment.

Teaching and Learning

Teaching and Learning is a collaborative process involving learners, lecturers and academic support staff. All students enrolled on this programme, are at the centre of this process, and their success depends on their active engagement with it. Below are some of the items students can expect from lecturers and academic support staff and some items we expect from students:

Students can expect the programme teaching and support staff to:

- Treat all learners with dignity and respect
- Provide academic support and guidance
- Provide appropriate teaching and learning materials
- Provide a Module Descriptor for each Module studied
- Assess your learning in ways that are fair, consistent and valid
- Assure fair and consistent enforcement of all College rules and procedures

In turn, Students are expected to:

- Treat all teaching and support staff and students with dignity and respect
- Take responsibility for their own learning
- Attend all classes tutorials and other learning sessions
- Make proper use of all learning resources provided
- Attempt honestly all assessments set on your programme
- Abide by all the programme‘s rules, regulations, and procedures

Teaching attempts to create a relevant and meaningful context for learners to make practical connections to the knowledge and skills being acquired. This is primarily achieved through the broadly practical nature of tutorials across most modules which expose students to industry-based technologies and techniques through practical laboratory exercises.

Teaching styles and contexts are flexible and aim to motivate and engage learners. Assessments are recognised as learning opportunities, and are designed to match the level of study, and to prepare learners for progression.

The part-time programs are delivered entirely online through Directed E-Learning (DEL), which combines on-demand activities and live online classes using virtual classroom technology. Students will complete specific tasks independently at scheduled times on the program's Learning Management System (LMS). This approach helps avoid overcrowded schedules, especially for students with limited time, and allows the program team to keep track of student progress and engagement in the online courses.

Asynchronous activities may consist of reading or audio/video-based content, as well as practical lab exercises which must be uploaded to the LMS on a periodicly. The synchronous class contact elements build upon and supplement the asynchronous and self-paced learning materials and activities on Moodle to create an environment whereby learners engage practically with materials outside of class time, leaving time for practical facilitation based directly on those materials in class-contact time.

For Full Time programmes, both lecture and practical labs/tutorials will be delivered fully online. Full Time learners will also be able to avail of DEL assets and resources.

Learners are also given the tools and guidance to create and manage their own digital spaces where they can organise group work/study groups/support chats etc.

In general, asynchronous activities consist of:

- Audio/Video presentations
- Podcasts
- Practical Lab/Project work

- Asynchronous discussion activities

Synchronous activities consist of:

- Live lectures
- Live labs
- Group work/Breakout rooms

Due to the fully online delivery mode, the programme team will ensure that:

- Learners are advised in advance of commencement of the programme of the technical requirements and pre-requisite skills for effective participation on the programme.
- Learners are provided with support during programme induction on how to use the learning technologies.
- Support and on-going professional development are provided to College staff in the design, production and use of new technologies in teaching and learning.
- Technical support is provided for the systems utilised by the programme (e.g., LMS, Learner Portal, etc.).
- Programme and module learning outcomes and associated assessments are the same for all modes of delivery except where specifically specified and approved.
- Lecturers are encouraged to apply good pedagogic design to their production and planning of learner learning activities – this is achieved by mapping such activities against specific learning outcomes.
- Learners should be provided with opportunities to review archived instructional sequences for revision purposes.
- Learner assignments are to be submitted electronically through the LMS unless otherwise specified.

Students should be aware that there is a clear link between attendance at, and engagement in learning sessions, and their performance in each of the modules.

Assessment

Teaching follows the principle of constructive alignment and hence establishes a close relationship between the intended learning outcome of a module, the teaching formats applied and the assessment methods. Exams are designed to assess the extent to which the defined learning objectives have been achieved. Module Descriptor documentation provides information on the types of exams and assessments (with possible alternatives) that are specified for each module. Learners are informed about the conditions for completing the module (coursework, exams etc.) at the beginning of each module. Examinations are marked according to transparent criteria. Grading rubrics for assignments are provided to learners. Lecturers will provide general assessment feedback regarding assignments in a timely manner (typically within two weeks of the assessment submission date). Learners may also apply for additional feedback meetings with their lecturers.

The rationale for the choice of assessment instrument follows five principles:

1. *Students are responsible for demonstrating their learning achievement*: A student who is enrolled on a programme should submit his or her assessment to demonstrate their attainment of the programme's intended learning outcomes.

2. *Assessment is designed to meet specific standards related to learning outcomes*: Grades and awards are given solely based on assessments that evaluate specific criteria, which include knowledge, skills, and competencies.
3. *Assessment promotes and supports effective learning and teaching*: Effective assessment is intrinsic to effective teaching and learning, and is (i) consistent with, (ii) supportive of, and (iii) derived from the intended programme and module learning outcomes.
4. *Assessment methods are regularly reviewed*: The Joint Programme Committee, in conjunction with the Quality Enhancement and Curriculum Development Committee, regularly review the assessment methods to adapt to evolving requirements. Each module's assessment strategy is designed to effectively evaluate the learning outcomes for that module.
5. *Students are well informed about how and why they are assessed*: Students need to be (i) familiar with and understand the intended module and programme learning outcomes, relevant programme and module assessment strategies and (ii) regularly reminded of the assessments and their regulations.

All modules use formative assessments as in-class individual or group activities to assess the learning progress of the students. Assessments can include practical lab work, completed during mentoring and tutoring hours to enhance hands-on learning. In addition, each individual module assessment strategy is composed of one or at most two additional assessments. The types of assessment may vary, but can include:

- Open book examinations/Terminal examinations where learners can demonstrate their understanding of the topic and their capacity to conduct research about the topic.
- Peer reviews where learners demonstrate their critical analysis skills. I
- Individual as well as team projects where learners can hone and demonstrate their practical and leadership skills

All examinations and assessments are conducted in accordance with the jointly agreed policies and procedures for the degree programme as adopted by the Master's Board of Directors. Each of the partner institutions has agreed on joint examination regulations for the programme. An agreed set of rules for conducting and organising examinations and assessments will be implemented for the programme. The Examinations Board is responsible for ensuring compliance with these regulations.

Documentation detailing the assessments and examinations rules and regulations are made available to students. Additionally, the Modules Handbook specifies the type of assessments associated with each of the programme's modules, including a breakdown of the contribution of each assessment to a module's overall marks and an indication of when the assessment will take place.

Learners can apply for a module repeat assessment in the case of initially failing a module. In such cases, the repeat assessment covers all learning outcomes associated with the failed module. If a learner subsequently fails a module after attempting a repeat assessment, it is then necessary for the learner to re-enrol for repeat attendance on the module.

Further information on examination and assessment of learners will be rendered available in the Study and Examination Regulation document available for download from the https://www.digital4security.eu.

Resits and Repeat Assessments

If a student receives an insufficient grade, misses, or withdraws from a module assessment or examination, they must retake it.

Late Submission of Coursework

Late submission of assignments is only accepted under special circumstances, e.g. illness. The student must inform the lecturer before the deadline of the assignment and should present medical proof on request to the Programme Coordinators team. If not, the lecturer can decide to sanction the student in terms of grading or refuse to accept late work. Assignments submitted late are typically graded as a failure.

Avoiding Problems with Plagiarism, Poor Scholarship, Collaboration/Collusion, Outsourcing Assessments, Knowingly aiding and abetting Academic Misconduct

Plagiarism

Plagiarism occurs when someone uses another person's work, whether text, graphics, tables, photographs, videos, music, or computer code, without proper acknowledgment. This includes failing to use quotation marks for direct quotes, not citing sources for paraphrased work, and not referencing any borrowed material. Additionally, submitting the same work for multiple assignments is also considered plagiarism, which is a serious violation. To avoid plagiarism, it's crucial to properly cite and reference all sources

Collaboration/Collusion

Where two or more students work together, without the prior authorisation of the course lecturer or supervisor, to produce the same piece of work, and then attempt to present this work as entirely their own work, is also a disciplinary offence.

Poor Scholarship

Poor scholarship may consist of poor referencing, but where there is clearly no intention to deceive. This may be penalised in the mark you receive. Poor scholarship may also consist of very close paraphrasing of published work, or the over-use of long quotations (such that your own contribution is unclear) and will also receive a low mark.

Cheating in assessments or examinations

Using, having, sharing, or relying on any unauthorised materials or help during any assessment or academic activity is considered a violation and may lead to disciplinary action

Outsourcing assessment

Having others complete assessments for oneself whether personally or via any free or commercial service is a disciplinary offence.

Knowingly aiding and abetting academic misconduct

Cases in which students knowingly permit others to copy all or part of their work shall also be subject to the procedures outlined here and considered an offence.

Plagiarism of software code

This policy relates to plagiarism of programming assignments that take place as continuous assessments in modules. All continuous assessments and projects are part of the examination process and any attempt to plagiarise is a major offence, punishable accordingly.

Plagiarism includes the following:

- Re-use of code that is based on the learning outcome of the module.
- Submitting another student's work as your own (with or without that person's consent).
- Any act designed to give a student an unfair advantage over another student or the attempt to commit such acts.
- Allowing another student to use your entire program code.
- The reuse of code from previous years' laboratory assessments.
- Not being able to demonstrate an awareness and understanding of the code.
- Taking code with no understanding and not tailoring it to the requirements of the assessment.
- Re-use of code from other locations and not substantially modifying it.

This policy advocates the use of software reuse under strict guidelines namely:

- Each source code program shall contain a standard header which states that this is entirely the authors own work or references the re-used code.

It is at the lecturer's discretion to determine whether a student has breached the above conditions and committed plagiarism.

Disciplinary Committee

Students found guilty of these offences will be penalised and may be reported to the Master's Board of Directors. The Master's Board of Directors may subsequently convene a Disciplinary Committee. Disciplinary measures include written warnings, suspension from the programme, or expulsion and exclusion of the student from the programme.

Student Mobility

As delivery of the programme is fully online, there will be no requirement for learners to physically attend classes at any partner institution's geographical location. Learner mobility will be virtual –

with learners enrolling on modules that will be delivered by faculty from the different institutional partners. In addition to this, learners will also have opportunities to attend various networking events. These events will be hosted by partner institutions in different countries as part of the programme's schedule.

The Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty Award

Students who have satisfied all the requirements of the final assessment shall be awarded the Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty.

Students who have not satisfied all the requirements of the final assessment within the duration of the degree programme will be required to re-register and pay extension fees.

The degree awarded shall be testified by the issuance of a Master's Degree and Diploma Supplement. The Diploma Supplement shall follow the template developed by the European Commission, the Council of Europe and UNESCO/CEPES and shall be adapted to any further specifications in national legislation where applicable. The Degree Certificate will be issued in the form of a Joint Degree.

Grading System

The Grading Scheme and Honours are outlined in Table 7.

Table 7: Classification of Honours in Relation to Point Average Boundaries

Classification of Master's Degree	Percentage Point Average Boundaries	Description
First-class honours	90%	Achievement includes that required for a Pass and in most respects is significantly and consistently beyond this.
Second-class honours	75%	Achievement includes that required for a Pass and in many respects is significantly beyond this.
Pass	60%	Attains all the minimum intended programme learning outcome.

Student Support Services

A student's principal supports on the programme are the academic and academic support staff (the Programme Coordinators). But since teaching and learning is a collaborative process, and since students may face a number of challenges during their time on the programme, a full range of further services are offered to students.

Information on the range of student support services can be found online through the student support services portal on the programme website. A number of student support services can be requested online through the student support services porta. The Programme Coordinators serve as the initial point of contact for processing such student's support requests. A variety of support services are available to help students enrolled in the program address their academic, personal, or professional challenges

Learning Development and Disability Support Service

The Learning Development and Disability Support Service aims to empower all students to become active and confident learners. This is accomplished through initial contact with students during the orientation process and the regular provision of effective academic skills throughout the programme's semesters.

To enhance this direct interaction, the service actively promotes the use of learning technologies and accommodates diverse learning preferences, creating an innovative and inclusive environment for all students. The aim of the Disability Support Service is to facilitate students in reaching their full potential by providing appropriate and specific support which meets individual needs. The programme is committed to provide equal access to education and equal opportunities for students with disabilities.

Careers and Opportunities Support Service

The programme incorporates an Employability Strategy. As part of this strategy, an extensive series of events will be scheduled to enhance the employability of students. These events will include online, hybrid, and on-site activities involving the Digital4Security consortium's industry partners and the wider business community. Moreover, the programme will provide a general Careers and Opportunities Service to facilitate and empower students in developing Career Management and Employability skills. The service also aims to assist students in exploring employment opportunities and/or graduate study options. This service provides a comprehensive and accessible Career Information Service for students and recent graduates.

Assistive Technology Support Service

The aim of the Assistive Technology (AT) Support Service is to dismantle the barriers to education for students with disabilities by harnessing the potential of technology. The AT Service promotes independent learning by providing technology and tailored training to meet the needs of individual students.

Student Counselling & Wellness Service

The Student Counselling and Wellness Service's aim is to support students and offer a supportive encouraging environment where students can talk about any struggles or difficulties they may be facing while they are completing their studies.

Deciding to undertake a Master's degree is a big step and this may feel daunting and students face many new challenges. These challenges may be academic, career, or even personal problems that can interfere with student's ability to take full advantage of their experience on the programme. Counselling can be a helpful and supportive place to start.

Counselling can offer students some time and space to explore any issues that may be of concern such as:

- Stress
- Anxiety
- Academic difficulties
- Relationship difficulties
- Depression
- Family issues
- Grief or bereavement
- Homesickness/loneliness
- Sexual/personal identity issues
- Physical assault/abuse
- Self-harm
- Eating disorders
- Addiction or substance use
- Confidence or self-esteem
- LGBTQ+ Support
- Autism/ADHD Support

Students can book an appointment with the Student Counselling and Wellness Service via sending an email message to counselling@Digital4Security.eu. Once a message is received, a counsellor will contact the student with an available appointment. Counselling sessions last for 40- 50 minutes. A counsellor will discuss the frequency and number of sessions with the student depending on their needs (usually weekly/bi-weekly and anywhere from 1 to 6 sessions).

Library Service

Library services are a key learning resource for students. Library services provide access to a wide range of scholarly publications. Much information (useful and otherwise) is now available on the web, and you will need to be familiar how to use it effectively and correctly. . Library services for the programme provide an extensive source of on-line resources, all of which are of the quality that students need for successful study. The library catalogue may be accessed online and is searchable in a number of ways: author, title, author and title (the most useful for a specific reference), keywords (very good for a search). Copies of principal books and articles specified in the reading list are available through the programme 's library services and each module's description document.

Student Complaints Procedures

Making a Complaint

The following process is designed to resolve concerns as speedily and effectively as possible. Most concerns can be addressed successfully through informal means (before writing a formal complaint); however, if informal resolution is unsuccessful, a formal process is available. This procedure is not to be used in cases where the learner is not satisfied with an assessment result or outcome of disciplinary actions. In these cases, relevant appeals processes should be used.

If a student has a concern, it is expected that the student will express it, and not do so via a third party. If the student names another person in expressing a concern, that other person has a right to know what is said about them as soon as possible, and who has raised the concern. Any fear of retaliation as a result of raising a concern will not be tolerated. Confidentiality will be maintained when appropriate. All concerns are taken seriously. It is assumed they are legitimate. If an expressed concern is found to be malicious the Master's Board of Directors may have to consider initiating disciplinary proceedings.

We will respectfully deal with each concern and deal with it in the context of our policies and resources.

There are five steps in expressing a concern:

- Step 1: Approach the person responsible for the student's concern.

  The student should first address concerns directly to the person responsible and attempt to resolve the matter informally

- Step 2: Approach the person responsible for the area about which the learner has the concern.

  This may be the Master's Board of Directors or the Programme Coordinators. Many concerns can be dealt with informally by explanation and discussion. If the student needs help in expressing their concern or is reluctant to approach the person(s) responsible, the student r can seek advice from the Programme Coordinators.

- Step 3: Make a formal complaint in writing.

  If it is not possible to resolve the student's concern informally by discussion and explanation the student can lodge a formal complaint with the Master's Board of Directors. A formal complaint must be made in writing.

  Please supply the following details in a letter:

  - The student's name and where the student can be contacted
  - The nature of the complaint
  - What action, if any, has already been taken by the student to attempt to resolve the concern
  - Any prior action taken by the programme's management in regard to this matter
  - Say what the student would expect to be done to resolve the their complaint

Please send the written formal complaint to the Programme Coordinators marking the complaint for the attention of the Master's Board of Directors.

- Step 4: Acknowledgement of the complaint.

  The student can expect to receive a written acknowledgement of the learner's complaint within 20 (twenty) working days of its receipt. The student can expect to be kept informed if there is undue delay in coming to a conclusion on the student's complaint. If the person dealing with the student's complaint thinks it would be better dealt with by someone else, or that it should be dealt with under some other procedure, the student will be informed.

- Step 5: Investigation of the complaint and response

  The student's complaint will be investigated as quickly as possible and the student will receive a written response upon completion of the investigation detailing what action, if any, is to be taken.

Appeals

If the student is still unsatisfied after the initial investigation, they can request that the Project Coordinator, or another appropriate person or group who has not previously handled the student's complaint, conduct a further investigation

Communication

Online Communication

Official notices will be sent to student email accounts only. Furthermore, the programme's information page on the LMS provides students with information about their programme and and programme resources such as the library services, career development information, and programme related events. Further supports can be accessed through the support pages on the student support section of the website.

Appendix: Guide to Academic Writing

Assessment during the programme, whether through essays or examinations, is intended to help students develop their knowledge, skills and critical faculties and is one way in which student progress can be assessed and what kind of additional help students may need. This guide informs students of what is expected in relation to the work they submit. It should help students with their academic essay writing techniques.

Guidelines on Essay Writing

The following guidelines are intended to help students prepare and write essays and should be used in addition to guidance provided in module outlines. Essays are intended to develop students' analytical powers, their ability to construct a coherent and logical argument, and their understanding of the varied literature available on a particular subject. The feedback

provided on essays should enable students to consistently develop and refine their critical faculties throughout the programme.

These following guidelines address the two main technical components of a good essay: structure and style.

Essay Structure

All students are advised to follow these guidelines on essay structure, before starting to write an essay. The structure should have three main components: an Introduction, a main part, and a conclusion. Note that it is not a requirement to use subheadings, although you may find these helpful in structuring your essay. The question should be is ‘‘addressed’ rather than ‘answered’, in an organised analytical argument. Observe the word limit (plus or minus 10%).

1. Introduction

This should cover the following:

- Discussion of title - your understanding of what the question is asking, and the definition of any relevant terms.
- Summary of your argument.
- Indication of your conclusion.

Be careful not to allow the introduction to become over-long. This wastes space in a relatively short essay.

2. Main part

The main part of the essay should focus on a few major themes, ideally three or four. Adding more can overwhelm the reader and make the essay seem like a list.

Instead of merely summarizing readings or lecture notes, students should use them to support and strengthen their arguments. Analysis should not be substituted with summaries. They should evaluate various theories and evidence if required by the essay topic. When personal experiences are included, they should serve to illustrate points within the argument, not replace analytical thinking

3. Conclusion

The conclusion consolidates and summarizes the major findings from the main part of the essay. It may also suggest potential implications of the argument. New material should not be introduced at this stage. Once the conclusion is clear, it can be integrated into the introduction, outlining the central argument at the start. This approach clarifies the subsequent discussion.

Constructing an essay plan before beginning the writing process is beneficial. The plan should outline the main points of the introduction, key themes from the main body, and the conclusions, including any resulting implications. This provides a clear roadmap for the essay. Students are advised to discuss their essay plans with the module lecturer for further refinement

Style

The following guidelines are not exhaustive but should help students with general and stylistic points. All essays must be referenced, with a bibliography at the end.

All concepts, figures and other evidence, use a deisgnated referencing system (e.g., Harvard, IEEE).

Bibliography - at the end of the essay, a Bibliography should be included where all references are listed in full according to the referencing system you are using.

Statistics - when referring to data and statistics, use rounded numbers in the text. For example, if the cited figure is 13,201, either put 13,000 or "just over 13,000". Unless there is a good reason, you should avoid decimal places - so put 49% rather than 48.8%.

Do not copy other student's essays. This is a disciplinary offence: see the section on 'Collaboration/ Collusion' in this Handbook.

Quotes - do not over-quote.

Compiling a series of quotations, no matter how relevant, does not replace the need to develop arguments in the essay writer's own words and with their own emphasis. A careful use of quotes that enhances the argument is sufficient. When quoting, writers should avoid long paragraphs and consider that often a single sentence or phrase captures the essential point. Inserting passages from literature without proper citation and acknowledgment can be viewed as plagiarism by the evaluator (refer to the 'Plagiarism' section in the HRM Handbook). When referencing an author's work, the full citation—author, date, and page—must be provided. Essays should not be comprised solely of paragraphs that start with phrases like 'Jones/Smith argues....' Instead, they should focus on concepts, issues, and cases, with references to the authors. Avoid assertions, vagueness, and value-judgements. For example:

- 'It is well known that' (assertion - statement without evidence)
- 'Some business leaders have said' (vague - imprecise statement)
- "unfortunately, Labour is still in government" (value-judgement)

Historical material - too much of this is often reproduced in essays. As with other evidence, it should be used selectively to illustrate arguments, not to avoid making them. In social science essays, historical exposition does not usually constitute an argument in its own right, so it should not be used as one of the major themes, but in support of each of the themes. Finally, historical material can easily impose its own structure on the writer - i.e. chronological - and, when reproduced, makes the essay far too descriptive, rather than analytical.

Check grammar and spelling. Do not use paragraphs either too short or too long; each should be a coherent unit.

Typing and Word-processing - Quite apart from the fact that a typed essay looks better and is easier to read, using word-processing facilities enables work to be corrected and altered without having to rewrite the entire essay. Any skills gained in typing and/or word-processing are almost certain to be useful in the workplace and a useful addition to student's CVs.

Disclaimer

The Digital4Security Consortium has made all reasonable efforts to ensure that the information contained within this publication is accurate and up-to-date when published but cannot accept responsibility for any errors or omissions.

The Digital4Security Consortium reserves the right to revise, alter or discontinue modules and to amend regulations and procedures at any time, but every effort will be made to notify interested parties.

Digital4Security
Shaping Europe's cyber future

IN VIEW OF THE COOPERATION AGREEMENT OF [INSERT DATE] BETWEEN THE BELOW-MENTIONED HIGHER EDUCATION INSTITUTIONS, MEMBERS OF THE DIGITALA4SECURITY CONSORTIUM JOINTLY DELIVER~~ING~~ THE

MASTER IN CYBERSECURITY MANAGEMENT & DATA SOVEREIGNTY,

[INSERT NAME], RECTOR OF GERMAN UNIVERSITY OF DIGITAL SCIENCE • [INSERT NAME], RECTOR OF MUNSTER TECHNOLOGICAL UNIVERSITY • [INSERT NAME], RECTOR OF UNIVERSITY OF RIJEKA • [INSERT NAME], RECTOR OF ~~UNIVERSIDAD INTERNACIONAL DE LA RIOJA~~UNIVERSITY OF LA RIOJA • [INSERT NAME], RECTOR OF UNIVERSITY OF KOBLENZ, DECLARE THAT:

[STUDENT'S FULL NAME]

concluded all the course units of the programme on the [INSERT DATE], with 120 credits (ECTS) obtained. All legal requirements having been complied with, authorization is given to issue this ***Diploma of Higher Education*** conferring the degree of ***Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty*** awarded jointly by the above mentioned institutions with a final classification of [NUMBER OF CREDITS] (in ECTS scale).

German University of Digital Science
[INSERT NAME]
_____

Munster Technological University
[INSERT NAME]
_____

University of Rijeka
[INSERT NAME]
_____

University of La Rioja
[INSERT NAME]
_____

University of Koblenz
[INSERT NAME]
_____

German University of Digital Science
UTM
FIDIT University of Rijeka Faculty of Informatics and Digital Technologies
unir LA UNIVERSIDAD EN INTERNET
uk university of koblenz continue discovering

Diploma Supplement

This Diploma Supplement model was developed by the European Commission, Council of Europe and UNESCO/CEPES. The purpose of the supplement is to provide sufficient independent data to improve the international 'transparency' and fair academic and professional recognition of qualifications (diplomas, degrees, certificates etc.). It is designed to provide a description of the nature, level, context, content, and status of the studies that were pursued and successfully completed by the individual named on the original qualification to which this supplement is appended. It should be free from any value judgements, equivalence statements or suggestions about recognition. Information in all eight sections should be provided. Where information is not provided, an explanation should give the reason why.

1. INFORMATION IDENTIFYING THE HOLDER OF THE QUALIFICATION

1.1 Family name(s)
[INSERT NAME]

1.2 First name(s)
[INSERT NAME]

1.3 Date of birth (dd/mm/yyyy)
[INSERT DATE]

1.4 Student identification number or code (if applicable)
[INSERT STUDENT ID]

2. INFORMATION IDENTIFYING THE QUALIFICATION

2.1 Name of qualification and (if applicable) title conferred (in original language)
Joint Master's Degree Programme in Cybersecurity Management & Data Sovereignty

2.2 Main field(s) of study for the qualification
Advanced Digital Skills / Digital Transformation / Technology

2.3 Name and status of degree-awarding institutions (in original language)

GERMAN UNIVERSITY OF DIGITAL SCIENCE GGMBH
MUNSTER TECHNOLOGICAL UNIVERSITY
SVEUCILISTE U RIJECI
UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA
UNIVERSITAT KOBLENZ

2.4 Name and status of institution (if different from 2.3) administering studies (in original language)

Contributing Higher Education Institutions (HEIs), in collaboration with HEIs from 2.3 (in original language)
UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE POLITEHNICA BUCURESTI
NATIONAL COLLEGE OF IRELAND
UNIVERSITA DEGLI STUDI DI BRESCIA
VYSOKE UCENI TECHNICKE V BRNE
POLITECNICO DI MILANO
VYTAUTO DIDZIOJO UNIVERSITETAS
MYKOLO ROMERIO UNIVERSITETAS
CY CERGY PARIS UNIVERSITE

2.5 Language(s) of instruction/examination
English

3. INFORMATION ON THE LEVEL AND DURATION OF THE QUALIFICATION

3.1 Level of the qualification
Master's programme (UNESCO ISCED Code 7)

3.2 Official duration of programme in credits and/or years
120 ECTS, two years (full-time) /3 years (part-time)

3.3 Access requirement(s)

- According to Admission Criteria section of the Study and Examination Regulations the admission requirements are:
  - Applicants are required to hold a minimum of an EFQ Level 6 honours qualification. Ideally, applicants for the programme will have some relevant work experience in industry. Previous numerical and computer proficiencies should be part of their work experience or formal training. Graduates from disciplines which do not have technical problem-solving skills embedded in their programme will need to be able to demonstrate technical proficiency and problem-solving skills in addition to their EQF Level 6 programme qualifications (Certifications, Additional Qualifications, Certified Experience and Assessment Tests).
  - As the programme delivery is fully online, applicants must also be in possession of the necessary computing equipment (e.g., laptop / desktop PC) with the minimum required

specification that will be communicated to each applicant as part of the admissions process. Additionally, applicants must ensure that they have access to internet services.
- Practical experience working in a business environment is valued.
- Practical experience in a scientific or technology domain is valued.
- All required application details, relevant information, and necessary documentation have been submitted by the applicant.
- Selection criteria include motivation, type and level of academic achievements and qualifications, level of language abilities, type and level of research experience, and level of professional experience.
- Applicants meet Recognition of Prior Learning (RPL) policy requirements (see section Recognition of Prior Learning Policy in the Study and Examination Regulations).

4. INFORMATION ON THE PROGRAMME COMPLETED AND THE RESULTS OBTAINED

4.1 Mode of study

Full Time / Part Time

4.2 Programme learning outcomes

- Critically assess and evaluate cybersecurity principles, practices, and technologies relevant to modern enterprises.
- Strategically apply cybersecurity knowledge and utilise practical skills and technologies for long-term success in cybersecurity leadership roles across diverse industries, government agencies, and institutional settings.
- Identify knowledge gaps and undertake self-learning to acquire new knowledge to support professional development and the ability to adapt to evolving threats, technologies, and regulatory environments.
- Exhibit and apply leadership skills necessary for effectively managing cybersecurity initiatives within organisations, including education and training, strategic planning, and resource allocation.
- Critically evaluate and analyse cyber threats in order to implement effective security operations, and to enable the proactive identification, assessment, and mitigation of cyber threats.
- Effectively apply analytical and strategic thinking in order to make decisions to address security requirements. Communicate effectively across a range of complex and advanced cybersecurity concepts to provide leadership within an organisation and facilitate effective collaboration and teamwork.
- Critically assess cybersecurity legal, information governance, and regulatory frameworks and practices to ensure effective oversight, auditing, risk mitigation, accountability, compliance, and strategic alignment with organisational objectives.

4.3 Programme details, individual credits gained and grades/marks obtained

See Final Examination Certificate incl. Transcript of Records.

4.4 Grading system and, if available, grade distribution table

The following table provides an informative mapping in national scales of the partner Institutions and transposed to the European Common Credit Transfer System scale.

ECTS Scale	FX, F Fail	E Sufficient	D Satisfactory	C Good	C Good	B Very Good	A Excellent
Universitatea Națională de Știință și Tehnologie Politehnica Bucuresti (Romania)	1 – 4	5	6	7	8	9	10
Sveuciliste U Rijeci (Croatia)	1 nedovoljan	2 dovoljan	-	-	3 dobar	4 vrlo dobar	5 izvrstan
- Vysoke Uceni Technicke V Brne (Czech)	> 3 nevyhověl	-	-	-	3 dobře	2 velmi dobře	1 výborně
Cy Cergy Paris Universite (France)	Insuffisant (< 10)	Passable (10 – 10,49)	Passable (10,5 – 10,99)	Assez bien (11,0 – 11,49)	Assez bien (11,5 – 12,49)	Bien (12,5–14,49)	Très bien (14,5–20,0)
German University of Digital Science Ggmbh Universitat Koblenz (Germany)	> 4,01	4,00 – 3,51	3,5 – 3,01	3,00 – 2,51	2,50 – 2,01	2,00 – 1,51	1,50 – 1,00
- National College of Ireland - Munster Technological University (Ireland)	< 25% Fail	25% – 39% Pass	40% – 44% 3rd pass	45% – 54% -	55% - 69% 2nd / II	70% - 84% 2nd / I	85%-100% I
Politecnico Di Milano (Italy)	≤ 17	18, 19	20 – 22	23-24	25-26	27, 28	29,30, 30+
Vytauto Didziojo Universitetas Mykolo Romerio Universitetas (Lituania)	< 4	5	6	7	8	9	10
- Universita Degli Studi Di Brescia - Universidad Internacional de la Rioja SA (Spain)	< 5 Suspenso	5,0 – 5,49 Aprobado	5,5 – 6,49 Aprobado	6,5 – 7,49 Notable	7,5 – 8,49 Notable	8,5 – 9,49 Sobresalient Excellent	9,5 – 10 Matricula de Honor

4.5 Overall classification of the qualification (in original language)

Overall grade: X

5. INFORMATION ON THE FUNCTION OF THE QUALIFICATION

5.1 Access to further study

Doctoral studies, postgraduate studies

5.2 Access to a regulated profession (if applicable)

Not applicable

6. ADDITIONAL INFORMATION

6.1 Additional information

6.2 Further information sources

- Further information for the UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE POLITEHNICA BUCURESTI at: https://upb.ro.
- Further information for the GERMAN UNIVERSITY OF DIGITAL SCIENCE GGMBH at: https://german-uds.de.
- Further information for the NATIONAL COLLEGE OF IRELAND at: https://www.ncirl.ie.
- Further information for the MUNSTER TECHNOLOGICAL UNIVERSITY at: https://www.mtu.ie.
- Further information for the UNIVERSITA DEGLI STUDI DI BRESCIA at: http://www.unibs.it.
- Further information for the VYSOKE UCENI TECHNICKE V BRNE at: https://www.vut.cz.
- Further information for the SVEUCILISTE U RIJECI at: https://uniri.hr.
- Further information for the POLITECNICO DI MILANO at: https://www.polimi.it.
- Further information for the UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA at: https://www.unir.net.
- Further information for the VYTAUTO DIDZIOJO UNIVERSITETAS at: https://www.vdu.lt.
- Further information for the MYKOLO ROMERIO UNIVERSITETAS at: https://www.mruni.eu.
- Further information for the CY CERGY PARIS UNIVERSITE at: https://www.cyu.fr.
- Further information for the UNIVERSITAT KOBLENZ at: https://www.mykaufzack.de.

Further information on the Joint Master's programme can be found at https://www.digital4security.eu

7. CERTIFICATION

This Diploma Supplement refers to the following original documents:

Document on the award of the academic degree [date]
Certificate [date]
Transcript of Records [date]
Certification Date: Chairwoman/Chairman,
Examination Committee
(Official Stamp/Seal)

8. NATIONAL HIGHER EDUCATION SYSTEMS

The information on the national higher education systems on the following pages provides a context for the qualification and the type of higher education institutions that awarded it.

A. GERMANY

INFORMATION ON THE GERMAN HIGHER EDUCATION SYSTEM[1]

1 Types of Institutions and Institutional Status

Higher education (HE) studies in Germany are offered at three types of Higher Education Institutions (HEI).[2]

- Universitäten (Universities) including various specialised institutions, offer the whole range of academic disciplines. In the German tradition, universities focus in particular on basic research so that advanced stages of study have mainly theoretical orientation and research-oriented components.
- Fachhochschulen (FH)/Hochschulen für Angewandte Wissenschaften (HAW) (Universities of Applied Sciences, UAS) concentrate their study programmes in engineering and other technical disciplines, business-related studies, social work, and design areas. The common mission of applied research and development implies an application-oriented focus of studies, which includes integrated and supervised work assignments in industry, enterprises or other relevant institutions.
- Kunst- und Musikhochschulen (Universities of Art/Music) offer studies for artistic careers in fine arts, performing arts and music; in such fields as directing, production, writing in theatre, film, and other media; and in a variety of design areas, architecture, media and communication.

Higher Education Institutions are either state or state-recognised institutions. In their operations, including the organisation of studies and the designation and award of degrees, they are both subject to higher education legislation.

2 Types of Programmes and Degrees Awarded

Studies in all three types of institutions have traditionally been offered in integrated "long" (one-tier) programmes leading to Diplom- or Magister Artium degrees or completed by a Staatsprüfung (State Examination).
Within the framework of the Bologna-Process one-tier study programmes have successively been replaced by a two-tier study system. Since 1998, two-tier degrees (Bachelor's and Master's) have been introduced in almost all study programmes. This change is designed to enlarge variety and flexibility for students in planning and pursuing educational objectives; it also enhances international compatibility of studies. The German Qualifications Framework for Higher Education Qualifications (HQR)[3] describes the qualification levels as well as the resulting qualifications and competences of the graduates. The three levels of the HQR correspond to the levels 6, 7 and 8 of the German Qualifications Framework for Lifelong Learning[4] and the European Qualifications Framework for Lifelong Learning[5].
For details cf. Sec. 4.1, 4.2, and 4.3 respectively. Table 1 provides a synoptic summary.

[1] This information covers only aspects directly relevant to purposes of the Diploma Supplement.
[2] Berufsakademien are not considered as Higher Education Institutions, they only exist in some of the Länder. They offer educational programmes in close cooperation with private companies. Students receive a formal degree and carry out an apprenticeship at the company. Some Berufsakademien offer Bachelor courses which are recognised as an academic degree if they are accredited by the Accreditation Council.

3 Approval/Accreditation of Programmes and Degrees

To ensure quality and comparability of qualifications, the organisation of studies and general degree requirements have to conform to principles and regulations established by the Standing Conference of the Ministers of Education and Cultural Affairs of the Länder in the Federal Republic of Germany (KMK).[6] In 1999, a system of accreditation for Bachelor's and Master's programmes has become operational. All new programmes have to be accredited under this scheme; after a successful accreditation they receive the seal of the Accreditation Council.[7]

4 Organisation and Structure of Studies

The following programmes apply to all three types of institutions. Bachelor's and Master's study programmes may be studied consecutively, at various higher education institutions, at different types of higher education institutions and with phases of professional work between the first and the second qualification. The organisation of the study programmes makes use of modular components and of the European Credit Transfer and Accumulation System (ECTS) with 30 credits corresponding to one semester.

4.1 Bachelor

Bachelor's degree programmes lay the academic foundations, provide methodological competences and include skills related to the professional field. The Bachelor's degree is awarded after 3 to 4 years.

The Bachelor's degree programme includes a thesis requirement. Study programmes leading to the Bachelor's degree must be accredited according to the Interstate study accreditation treaty.[3]

First degree programmes (Bachelor) lead to Bachelor of Arts (B.A.), Bachelor of Science (B.Sc.), Bachelor of Engineering (B.Eng.), Bachelor of Laws (LL.B.), Bachelor of Fine Arts (B.F.A.), Bachelor of Music (B.Mus.) or Bachelor of Education (B.Ed.).

The Bachelor's degree corresponds to level 6 of the German Qualifications Framework / European Qualifications Framework.

[3] German Qualifications Framework for Higher Education Degrees. (Resolution of the Standing Conference of the Ministers of Education and Cultural Affairs of the Länder in the Federal Republic of Germany of 16 February 2017).

[4] German Qualifications Framework for Lifelong Learning (DQR). Joint resolution of the Standing Conference of the Ministers of Education and Cultural Affairs of the Länder in the Federal Republic of Germany, the German Federal Ministry of Education and Research, the German Conference of Economics Ministers and the German Federal Ministry of Economics and Technology (Resolution of the Standing Conference of the Ministers of Education and Cultural Affairs of the Länder in the Federal Republic of Germany of 15 November 2012). More information at www.dqr.de

[5] Recommendation of the European Parliament and the European Council on the establishment of a European Qualifications Framework for Lifelong Learning of 23 April 2008 (2008/C 111/01 – European Qualifications Framework for Lifelong Learning – EQF).

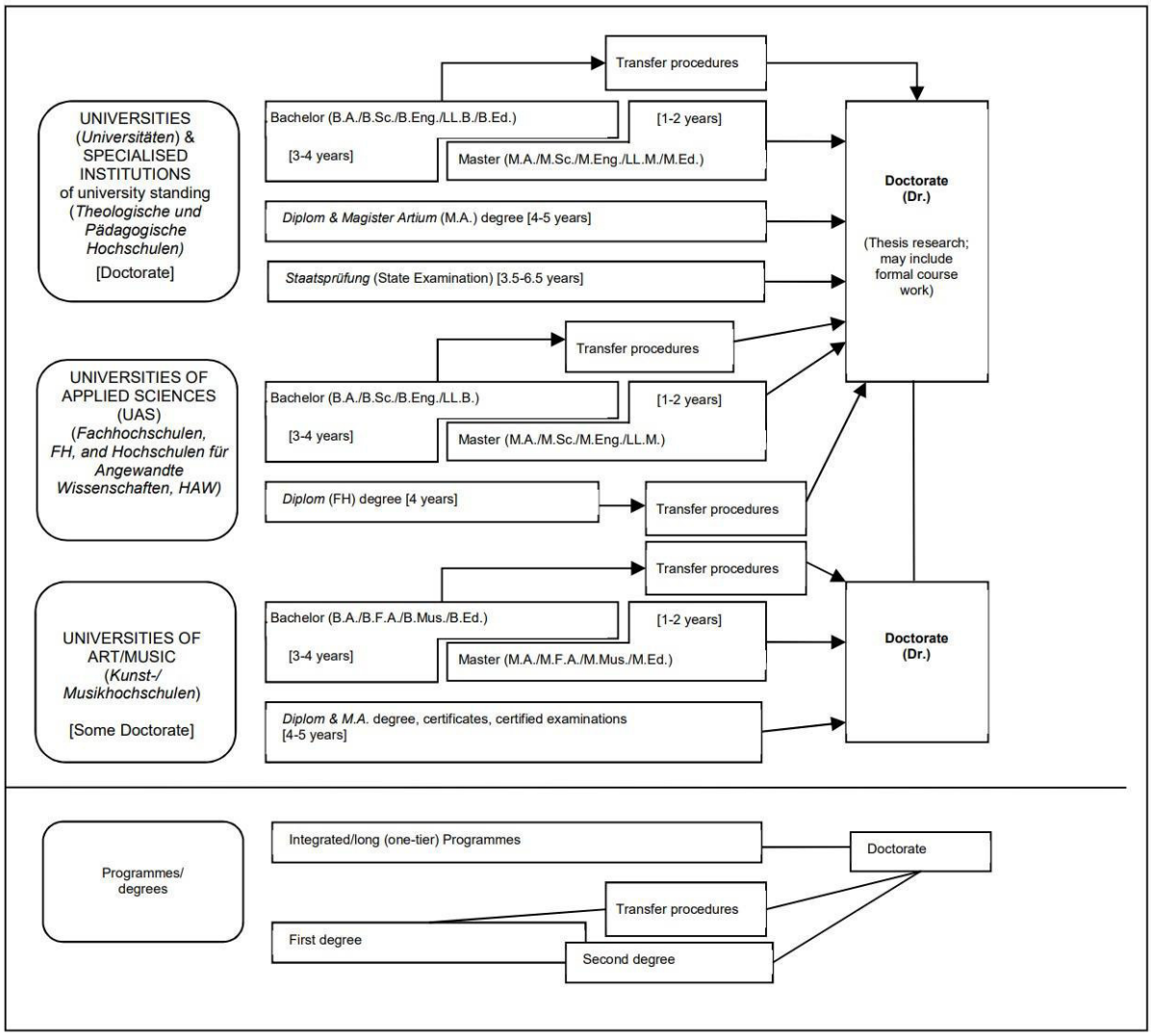
[6] Specimen decree pursuant to Article 4, paragraphs 1 – 4 of the interstate study accreditation treaty (Resolution of the Standing Conference of the Ministers of Education and Cultural AKairs of the Länder in the Federal Republic of Germany of 7 December 2017).

[7] Interstate Treaty on the organization of a joint accreditation system to ensure the quality of teaching and learning at German higher education institutions (Interstate study accreditation treaty) (Decision of the Standing Conference of

[3] See note No. 7.

the Ministers of Education and Cultural AKairs of the Länder in the Federal Republic of Germany of 8 December 2016), Enacted on 1 January 2018.

Table 1: Institutions, Programmes and Degrees in German Higher Education



4.2 Master

Master is the second degree after another 1 to 2 years. Master's programmes may be differentiated by the profile types "practice-oriented" and "research-oriented". Higher Education Institutions define the profile.

The Master's degree programme includes a thesis requirement. Study programmes leading to the Master's degree must be accredited according to the Interstate study accreditation treaty.[4]

Second degree programmes (Master) lead to Master of Arts (M.A.), Master of Science (M.Sc.), Master of Engineering (M.Eng.), Master of Laws (L.L.M.), Master of Fine Arts (M.F.A.), Master of Music (M.Mus.) or Master of Education (M.Ed.). Master´s programmes which are designed for continuing education may carry other designations (e.g. MBA).

The Master's degree corresponds to level 7 of the German Qualifications Framework / European Qualifications Framework.

[4] See note No. 7.

4.3 Integrated "Long" Programmes (One-Tier): Diplom degrees, Magister Artium, Staatsprüfung

An integrated study programme is either mono-disciplinary (Diplom degrees, most programmes completed by a Staatsprüfung) or comprises a combination of either two major or one major and two minor fields (Magister Artium). The first stage (1.5 to 2 years) focuses on broad orientations and foundations of the field(s) of study. An Intermediate Examination (Diplom-Vorprüfung for Diplom degrees; Zwischenprüfung or credit requirements for the Magister Artium) is prerequisite to enter the second stage of advanced studies and specialisations. Degree requirements include submission of a thesis (up to 6 months duration) and comprehensive final written and oral examinations. Similar regulations apply to studies leading to a Staatsprüfung. The level of qualification is equivalent to the Master's level.

- Integrated studies at Universitäten (U) last 4 to 5 years (Diplom degree, Magister Artium) or 3.5 to 6.5 years (Staatsprüfung). The Diplom degree is awarded in engineering disciplines, the natural sciences as well as economics and business. In the humanities, the corresponding degree is usually the Magister Artium (M.A.). In the social sciences, the practice varies as a matter of institutional traditions. Studies preparing for the legal, medical and pharmaceutical professions are completed by a Staatsprüfung. This applies also to studies preparing for teaching professions of some Länder.

The three qualifications (Diplom, Magister Artium and Staatsprüfung) are academically equivalent and correspond to level 7 of the German Qualifications Framework / European Qualifications Framework. They qualify to apply for admission to doctoral studies. Further prerequisites for admission may be defined by the Higher Education Institution, cf. Sec. 5.

- Integrated studies at Fachhochschulen (FH)/Hochschulen für Angewandte Wissenschaften (HAW) (Universities of Applied Sciences, UAS) last 4 years and lead to a Diplom (FH) degree which corresponds to level 6 of the German Qualifications Framework / European Qualifications Framework. Qualified graduates of FH/HAW/UAS may apply for admission to doctoral studies at doctorate-granting institutions, cf. Sec. 5.

- Studies at Kunst- and Musikhochschulen (Universities of Art/Music etc.) are more diverse in their organisation, depending on the field and individual objectives. In addition to Diplom/Magister degrees, the integrated study programme awards include certificates and certified examinations for specialised areas and professional purposes.

5 Doctorate

Universities as well as specialised institutions of university standing, some of the FH/HAW/UAS and some Universities of Art/Music are doctorate-granting institutions. Formal prerequisite for admission to doctoral work is a qualified Master's degree (UAS and U), a Magister degree, a Diplom, a Staatsprüfung, or a foreign equivalent. Comparable degrees from universities of art and music can in exceptional cases (study programmes such as music theory, musicology, pedagogy of arts and music, media studies) also formally qualify for doctoral work. Particularly qualified holders of a Bachelor's degree or a Diplom (FH) degree may also be admitted to doctoral studies without acquisition of a further degree by means of a procedure to determine their aptitude. The universities respectively the doctorate-granting institutions regulate entry to a doctorate as well as the structure of the procedure to determine aptitude. Admission further requires the acceptance of the Dissertation research project by a professor as a supervisor.

The doctoral degree corresponds to level 8 of the German Qualifications Framework / European Qualifications Framework.

6 Grading Scheme

The grading scheme in Germany usually comprises five levels (with numerical equivalents; intermediate grades may be given): "Sehr Gut" (1) = Very Good; "Gut" (2) = Good; "Befriedigend" (3) = Satisfactory; "Ausreichend" (4) = Sufficient; "Nicht ausreichend" (5) = NonSufficient/Fail. The minimum passing grade is "Ausreichend" (4). Verbal designations of grades may vary in some cases and for doctoral degrees. In addition, grade distribution tables as described in the ECTS Users' Guide are used to indicate the relative distribution of grades within a reference group.

7 Access to Higher Education

The General Higher Education Entrance Qualification (Allgemeine Hochschulreife, Abitur) after 12 to 13 years of schooling allows for admission to all higher educational studies. Specialised variants (Fachgebundene Hochschulreife) allow for admission at Fachhochschulen (FH)/Hochschulen für Angewandte Wissenschaften (HAW) (UAS), universities and equivalent higher education institutions, but only in particular disciplines. Access to study programmes at Fachhochschulen (FH)/Hochschulen für Angewandte Wissenschaften (HAW) (UAS) is also possible with a Fachhochschulreife, which can usually be acquired after 12 years of schooling. Admission to study programmes at Universities of Art/Music and comparable study programmes at other higher education institutions as well as admission to a study programme in sports may be based on other or additional evidence demonstrating individual aptitude.

Applicants with a qualification in vocational education and training but without a schoolbased higher education entrance qualification are entitled to a general higher education entrance qualification and thus to access to all study programmes, provided they have obtained advanced further training certificates in particular state-regulated vocational fields (e.g. Meister/Meisterin im Handwerk, Industriemeister/in, Fachwirt/in (IHK), Betriebswirt/in (IHK) and (HWK), staatlich gebrüfte/r Techniker/in, staatlich geprüfte/r Betriebswirt/in, staatlich geprüfte/r Gestalter/in, staatlich geprüfte/r Erzieher/in). Vocationally qualified applicants can obtain a Fachgebundene Hochschulreife after completing a stateregulated vocational education of at least two years' duration plus professional practice of normally at least three years' duration, after having successfully passed an aptitude test at a higher education institution or other state institution; the aptitude test may be replaced by successfully completed trial studies of at least one year's duration.[5]

Higher Education Institutions may in certain cases apply additional admission procedures.

8 National Sources of Information

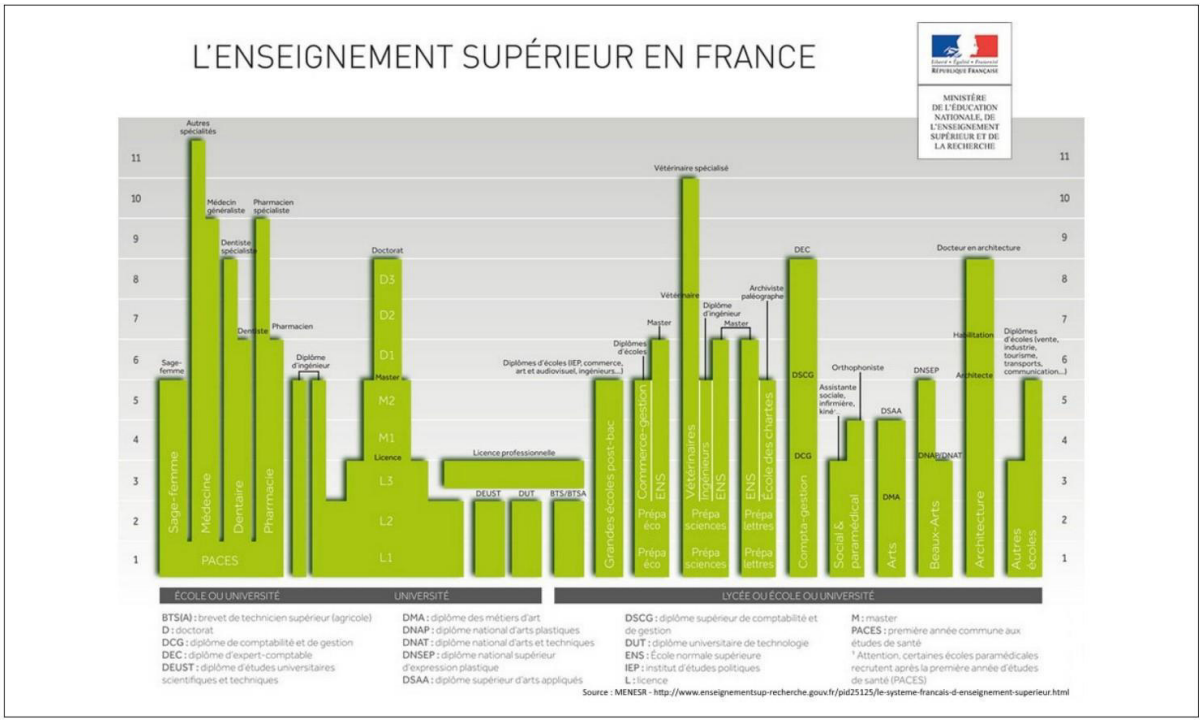
- Kultusministerkonferenz (KMK) [Standing Conference of the Ministers of Education and Cultural Affairs of the Länder in the Federal Republic of Germany]; Graurheindorfer Str. 157, D-53117 Bonn; Phone: +49[0]228/501-0; www.kmk.org; E-Mail: hochschulen@kmk.org
- Central Office for Foreign Education (ZAB) as German NARIC; www.kmk.org; E-Mail: zab@kmk.org
- German information office of the Länder in the EURYDICE Network, providing the national dossier on the education system; www.kmk.org; E-Mail: Eurydice@kmk.org -

[5] Access to higher education for applicants with a vocational qualification, but without a school-based higher education entrance qualification (Resolution of the Standing Conference of the Ministers of Education and Cultural AKairs of the Länder in the Federal Republic of Germany of 6 March 2009).

Hochschulrektorenkonferenz (HRK) [German Rectors' Conference]; Leipziger Platz 11, D-10117 Berlin, Phone: +49 30 206292-11; www.hrk.de; E-Mail: post@hrk.de

- "Higher Education Compass" of the German Rectors' Conference features comprehensive information on institutions, programmes of study, etc. (www.higherhttp://www.higher-education-compass.de/education-compass.de)

B. FRANCE



c) Portugal

System of Basic and Secondary Education:

The Comprehensive Law on the Education System (Law nº. 46/86, of 14 October, subsequently amended in respect of specific clauses by Law nº. 115/97, of 19 September) establishes the framework for the education system.

School education encompasses the following stages of teaching: basic, secondary and higher education. Pre-school education is optional and designed for children between the ages of three and the age for admission to the first cycle of basic education. Preschool education is run free in nursery classes of the public sector supported by the Ministry of Education (with the collaboration of regional or local authorities) and other public or private organisations.

Basic education is universal, compulsory, free, and consists of 3 consecutive cycles. The first cycle lasts for 4 years, the second for 2 years, and the third for 3 years.

Secondary education is not compulsory and it comprises a 3-years cycle (10th, 11th and 12th years of schooling).

Permeability is guaranteed between courses mainly geared to working life (technology courses) and those mainly geared to continued studies (general courses).

General Admission Requirements

Access to higher education is subject to numerous clauses.
To qualify for admission to higher education through the national competition, students are required to:

- Have successfully completed the 12th year of schooling or equivalent;
- Have completed the national-specific examinations in accordance with the higher education course the student wishes to attend;
- Have obtained a minimum mark when required;
- Have fulfilled the prerequisites for the higher education course the student wishes to attend, if required.

C. IRELAND

Description of the Higher Education and Training System in Ireland

The Irish system of higher education and training comprises a range of higher education institutions. The universities (including linked colleges and colleges of education), Technological Universities, the Royal College of Surgeons of Ireland (RCSI), and the Institutes of Technology are established in law as designated awarding bodies. A range of private and other education and training institutions also deliver programmes leading to QQI awards. A list of recognised Higher Education Institutions can be accessed on Higher Education Institutions in Ireland https://www.gov.ie/en/publication/5088c-list-ofhttps://www.gov.ie/en/publication/5088c-list-of-publicly-funded-higher-education-institutions/publicly-funded-higher-education-institutions/.

Government Agencies

While overall responsibility for the education and training system lies with the Department of Education and Skills (www.education.ie), there are several state agencies with responsibility for specific functions in higher education. The Higher Education Authority (www.hea.ie) is responsible for furthering the development and assisting in the coordination of State investment in higher education and training, including research and international education.
Quality and Qualifications Ireland (www.qqi.ie) is responsible for the National Framework of Qualifications (NFQ) and for the external quality assurance of further and higher education and training (including English language provision).

The National Framework of Qualifications

The types and expected learning outcomes of national awards made by higher education institutions at undergraduate and postgraduate level are described in the National Framework of Qualifications (NFQ). The Framework has ten levels, which include awards made by schools, further and higher education and training institutions. Awards in the NFQ are nationally and internationally recognised and are underpinned by legislative quality assurance arrangements. There are overarching level indicators at each of the 10 levels of the Framework with associated sub-strands of knowledge, skill and competence appropriate to the achievement of an award at each of these levels. The NFQ is aligned with the Bologna Framework (Framework for Qualifications of the European Higher Education Area) and is referenced to the European Qualifications Framework for Lifelong Learning (EQF).

Each Major and Higher Education Award is Described Below

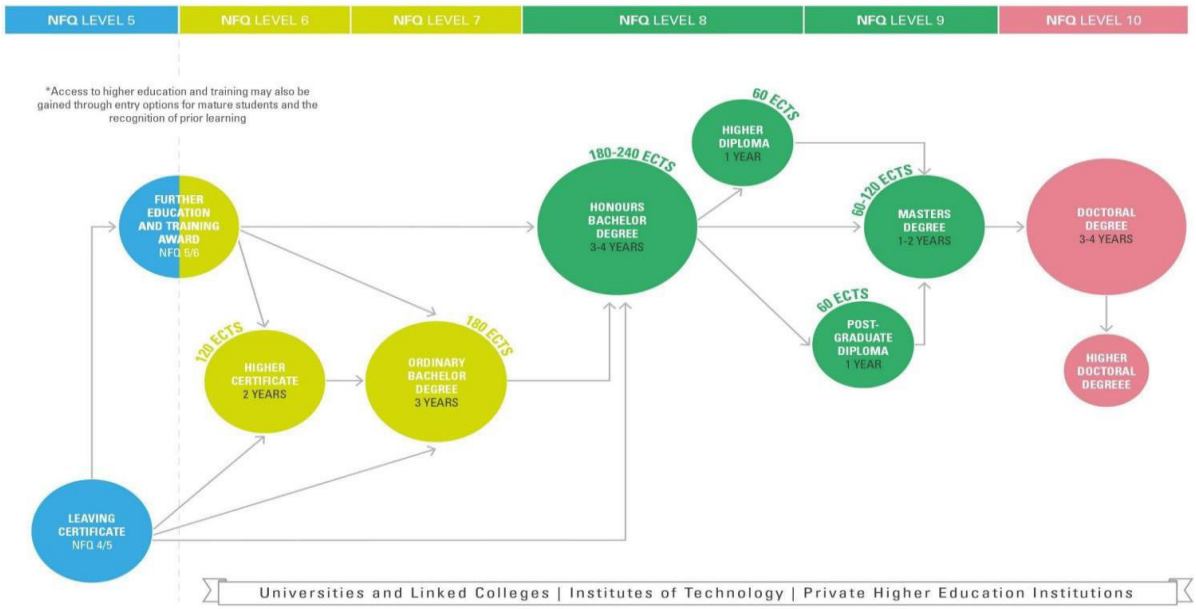
HIGHER CERTIFICATE (NFQ LEVEL 6 / EQF LEVEL 5)	The Higher Certificate is normally awarded after completion of a programme of two years duration (120 ECTS credits). Entry to these programmes is generally for school leavers and those with equivalent qualifications. The Higher Certificate is an intermediate qualification within the Bologna First Cycle.
ORDINARY BACHELOR DEGREE (NFQ LEVEL 7 / EQF LEVEL 6)	The Ordinary Bachelor Degree is normally awarded after completion of a programme of three years duration (180 ECTS credits). Entry to a programme leading to an Ordinary Bachelor degree is typically for school leavers and those with

	equivalent qualifications. In addition, there are transfer arrangements in place across higher education and a number of programmes of one-year duration leading to the Ordinary Bachelor Degree for holders of the Higher Certificate. The Ordinary Bachelor Degree is compatible with the Bologna First Cycle descriptor, though holders of this award do not generally immediately access programmes leading to Second Cycle awards in Ireland.
HONOURS BACHELOR DEGREE (NFQ LEVEL 8 / EQF LEVEL 6)	The Honours Bachelor Degree is normally awarded following completion of a programme of three to four years duration (180-240 ECTS credits), although there are examples of longer programmes in areas such as architecture, dentistry and medicine. Entry is generally for school leavers and those with equivalent qualifications. In addition, there are transfer arrangements across higher education, and a number of programmes of one-year duration leading to Honours Bachelor Degrees for holders of the Ordinary Bachelor Degree. The Honours Bachelor Degree is a Bologna First Cycle qualification.
HIGHER DIPLOMA (NFQ LEVEL 8 / EQF LEVEL 6)	The Higher Diploma is normally awarded following completion of a programme of one-year duration (60 ECTS credits). Entry to a programme leading to a Higher Diploma is typically for holders of Honours Bachelor Degrees but can also be for holders of Ordinary Bachelor Degrees. It is of note that the Higher Diploma is typically in a different field of learning than the initial award. The Higher Diploma is a qualification at the same level as completion of the Bologna First Cycle.

MASTERS DEGRE (NFQ LEVEL 9 / EQF LEVEL 7)	There are two types of Master's Degree in Ireland: taught Masters Degrees and research Masters Degrees. The taught Master's Degree is awarded following the completion of a programme of one to two- years duration (60-120 ECTS credits). Entry to a programme leading to a taught Master's Degree is typically for holders of Honours Bachelor Degrees. In some cases, entry to such programmes can be permitted for those with Ordinary Bachelor Degrees or equivalent. Research Master's Degree programmes are typically of two years duration (120 ECTS credits) though not all such programmes are credit-rated. The Irish Master's Degree is compatible with completion of the Bologna Second Cycle.
POST GRADUATE DIPLOMA	The Postgraduate Diploma is normally awarded following completion of a programme of one-year duration (60 ECTS credits). Entry to a programme leading to a Postgraduate.

(NFQ LEVEL 9 / EQF LEVEL 7)	Diploma is typically for holders of Honours Bachelor Degrees but can also be for holders of Ordinary Bachelor Degrees. The Postgraduate Diploma is an intermediate qualification within the Bologna Second Cycle.
DOCTORAL DEGREE (NFQ LEVEL 10 / EQF LEVEL 8)	Possession of an Honours Bachelor Degree is normally required for entry to a doctoral programme. In some disciplines, a Master's Degree is also preferred. Normally those entering a doctoral programme with an Honours Bachelor Degree initially register for a research Master's Degree or provisional doctoral candidature. Upon successful completion of this initial stage, the candidate acquires full doctoral candidature. Doctoral programmes are between three and four years in duration. ECTS credits are used in doctoral programmes for taught elements only. Varying doctoral programmes now exist, including professional and performance/practice-based doctorates. The Irish Doctoral Degree is compatible with completion of the Bologna Third Cycle.
HIGHER DOCTORATE (NFQ LEVEL 10 / EQF LEVEL 8)	This award largely recognises excellent and distinguished contributions to learning. It may be used for career progression to advanced levels of academia and research. This award is never based on a provider's programme and, as such, is not subject to validation but is assessed by the awarding body for each individual provider. Normally, the learner already holds a first doctorate or equivalent for some period of time prior to becoming a candidate for the higher doctorate. The Irish Higher Doctorate is compatible with completion of the Bologna Third Cycle.

HIGHER EDUCATION AND TRAINING SYSTEM



D. ROMANIA

According to the Law of National Education (Law 199/2023) universities and other higher education institutions are autonomous and have the right to establish and implement their own development policies, within the general provisions of the in-force legislation.
The Ministry of Education coordinates the activity of the universities and other higher education institutions, complying with their autonomy.
The university autonomy is correlated with the principle of personal and public accountability for the quality of the entire teaching and scientific research activity accomplished by the higher education institution. The university autonomy encompasses the domains of management, structuring and functioning of the higher education institutions, teaching and scientific research activities, administration and financing.
From the financing point of view, the university autonomy is accomplished through **the right to manage the funds** from the state-budget and other sources, according to the provisions of the law and personal accountability. Public higher education is financed from the state budget based on financing contracts signed between the Ministry of Education and the higher education institutions.
The entire **material basis** of higher education is the property of and administrated by the higher education institutions.
In Romania the national education system has an **open character**.
At the higher education level, the open character is ensured through the **University Charter.**
Higher education is accomplished through:

- Universities
- Academies of study institutions, and
- Post-university studies institutions.

The mission of the higher education institutions is:

- Either education and research, or
- Only education.

Specialisations and specialisations groups' **nomenclature** are established by the Ministry of Education in cooperation with the Ministry of Labour, Social Solidarity and Family, the higher education institutions as well as other interested players.
Higher education institutions usually include:

- Several faculties
- University colleges - colegiu universitar
- Departments
- Chairs, and
- Units for scientific research, design and micro-production.

The enrolment quota financed from the state/local budget(s) for all education levels is established yearly through Decisions of the Government.
According to the Law of National Education (Law 1/2011), only high school graduates holding a diploma de bacalaureat can be admitted in higher education. The higher education institutions establish **the admission methodology**, according to the general criteria established by the Ministry of Education.
The selection and admission procedure can rely on:

- The average mark obtained by the candidates at the national exam – examenul de bacalaureat and at various subjects studied during high school, as well as

- The mark obtained at an entrance examination entirely organised by the higher education institution.

Higher education institutions are authorized to accept a number of students exceeding the number of placements financed from the state-budget, subject to students' agreement to support the costs for the education provided (Law 441/2001).
All **students benefit** of:

- Free medical and psychological assistance in universities' or other public medical and psychological units.
- 50% reduction of the cost for internal public transportation (except air-travel) as well as for entrances to museums, concerts, theatres, opera, movies and other cultural and sports events organised by public institutions.
- Orphaned students benefit of free internal public transportation (except air-travel).

As for all education levels, scholarships and other forms of financial/material support are granted according to specific criteria.
Starting with 2005/06 academic year, all higher education institutions, private and public, are obliged by the 2004 Law to implement the new 3-cycle structure:

- **Bachelor**
- **Master** and
- **Doctorate**.

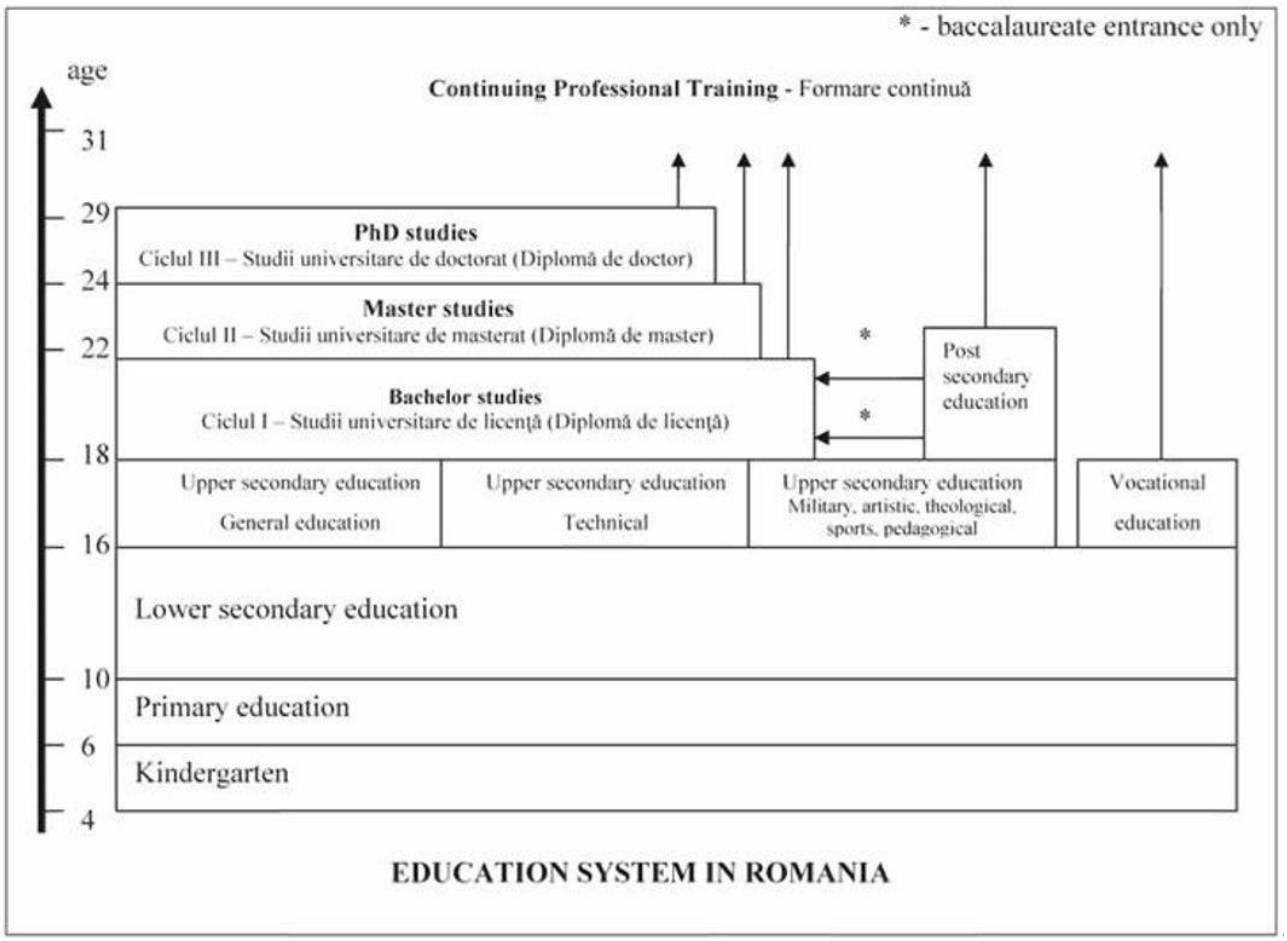
Each cycle has its own admissions and graduation procedures.
Special norms concerning the study conditions applicable to regulated professions adopted at European level have been established within the Romanian higher education system:

- **The first (Bachelor's) cycle** includes a minimum of 180 and a maximum of 240 transferable study credits equivalent to ECTS, and lasts three to four years, depending on the field and area of specialisation.
- **The second, Master** includes a minimum of 60 and a maximum of 120 transferable study credits (in exceptional cases and depending on the length of the first cycle) and lasts one to two years.
- Both cycles should enable the accumulation of at least 300 transferable study credits.

The in-force legislation consents to and provides the general framework for the establishment of **private education institutions** of all levels, including universities and other higher education institutions.
In order to be recognised as part of the national education system, private education institutions have to be accredited through specific procedures established by the law. Diplomas and certificates emitted by the accredited private education institutions produce the same effects as the ones emitted by the public education institutions.
The persons belonging to the **national minorities** have the right to study and be instructed in their mother tongue at all levels and forms of education as well as in all types of education – providing there is a sufficient demand.

- **Study lines in Hungarian and German** for students belonging to these national minorities are organised in several higher education institutions.
- Certain higher education institutions organise departments for initial teacher training for **teaching the languages of national minorities** in Pre-tertiary education.

- At the same time, the Law of National Education (Law 1/2011) states that **learning of Romanian**, as the official language, is compulsory for all Romanian citizens, irrespective of their nationality.



E. SPAIN

Higher education is integrated by:

- University education;
- Some programmes in non-university education:
  - Advanced vocational training;
  - Most of the programmes in artistic education (in particular, advanced plastic arts and design professional studies and advanced arts studies) and advanced sports education. These are all part of the specialised education programmes.

University education is regulated by Organic Law 2/2023 on the University System (LOSU). The rest of the studies are regulated by Organic Law 2/2006 on Education (LOE), as amended by Organic Law 3/2020 (LOMLOE).

Higher education qualifications correspond to the levels and qualifications established in the Spanish Qualifications Framework for Higher Education (MECES) and to the levels established in the European Qualifications Framework:

Spanish Qualifications Framework for Higher Education			European Qualifications Framework
LEVELS		**QUALIFICATIONS**	**LEVELS**
1	Advanced Technician	Vocational Training Advanced Technician Advanced Technician in Plastic Arts and Design Advanced Technician in Sports	Level 5
2	Bachelor's	Bachelor's Degree Advanced Degree in Glass; in Ceramics; in Conservation and Restoration of Cultural Heritage; in Design.	Level 6
3	Master's	Master's Degree Advanced Degree in Music in all its specialities Advanced Degree in Dance in all specialities Advanced Degree in Dramatic Art Master's Degree in Artistic Education Bachelor's Degree of at least 300 ECTS credits including at least 60 ECTS credits at Master's level, which has obtained this level of qualification by resolution of the Council of Universities	Level 7
4	PhD	Doctoral Degree	Level 8

Source: Drawn up by Eurydice España-REDIE (INEE, MEFD) based on Royal Decree 1027/2011 and its subsequent amendments.

University Education

Structure

University education is organised into bachelor, master and PhD programmes.

General Objectives and Functions

The university system is granted with the development of a public service of higher education through teaching, research, and knowledge transfer. Universities are endowed with **legal personality** and carry out their functions in a system of autonomy by virtue of the fundamental right recognised in Article 27.10 of the Spanish Constitution.

It has the following **functions**:

- Education and training of students through the creation, development, transmission and critical evaluation of scientific, technological, social, humanistic, artistic and cultural knowledge, as well as the capacities, competences and skills inherent to it;
- Preparation for the exercise of professional activities that require the application and updating of scientific, technological, social, humanistic and cultural knowledge and methods, as well as for artistic creation;
- Generation, development, dissemination, transfer and exchange of knowledge and the applicability of research in all scientific, technological, social, humanistic, artistic and cultural fields;
- Promotion of innovation based on knowledge in the social, economic, environmental, technological and institutional spheres;
- Contribution to social welfare, economic progress and the cohesion of society and the territorial environment in which they are located, as well as the promotion of their official languages, through training, research, transfer and exchange of knowledge and the culture of entrepreneurship, both individual and collective, based on conventional corporate models or social economy formulas;
- Generation of spaces for the creation and dissemination of critical thinking;
- Transfer and exchange of knowledge and culture within society as a whole through university activity and lifelong learning for all citizens;
- Training of citizens through the transmission of democratic values and principles;
- Encouraging the participation of the university community and citizens in activities promoted by voluntary and third sector organisations that are aligned with the principles and values of the university system;
- Other functions legally assigned to them.

Law 2/2011 on Sustainable Economy (Article 60) establishes that the university system must aim to achieve the following **general objectives**:

- Facilitate, through education, the acquisition of the qualifications demanded by the productive sector and by the public sector, and to improve adaptability to social and economic changes and, in general, the capacity to face long-term challenges;
- Promote the quality, competitiveness and internationalisation of universities through research training specialisation, modernisation of their infrastructures and improved efficiency in their management, with a reinforced commitment to the European Higher Education Area and the European Research Area (ERA);
- Foster scientific productivity, transfer of knowledge, technological development and innovation in all branches of knowledge;
- Facilitate university governance, by means of promoting measures which guarantee the exercise of government and managerial functions, the review of internal management and

governance procedures and the implementation of good practices in accordance with internationally recognised criteria of quality and efficiency in management;
- Increase transparency, internal control of finances and budgetary balance, as well as an external evaluation of their activity;
- Encourage talent recruitment, international mobility and collaboration with international reference universities and research institutions;
- Promote measures to attract private national and international investment, so as to contribute to the financing of the objectives of the university, especially in the area of research, transfer of knowledge and creation of innovation and technology-based business projects.

Structure of the Academic Year

Each university designs every year the organisation of the academic year.
As a general rule, the university school year establishes between 130 and 150 school days, excluding exam periods, organised in two semesters.
Universities, at their discretion, hold extraordinary examinations in June or July. Some universities hold their extraordinary exam sittings after the end of the corresponding ordinary sittings in each semester.

Schools Providing University Education

University education is provided by universities, which may be public or private.

Politics in University Education

The priority objectives of Spanish policy for university education are the following:
- Guaranteeing the fundamental right to education, as well as equity and equal opportunities in access to and permanence in the Spanish education system;
- Re-qualification of teaching and research staff;
- Promoting scientific and technical research and innovation in all sectors;
- Promoting the internationalisation of the Spanish university system;
- Digitalisation of the Spanish university system.

Non-University Education

Advanced Vocational Training

Vocational training consists of a set of training actions that enable the qualified performance of various professions, access to employment and active participation in social, cultural and economic life.
Vocational training is a priority area within the education and economic policy of Spain, and has become one of its main action lines. An ambitious package of reforms in legislation introduced a series of important changes in this type of provision, so as to contribute to adapt the training offer to the demands of the different productive sectors, to increase the educational offer, to advance towards the integration of vocational training in the education system, and to strengthen the cooperation between the different education authorities, as well as with other social agents and with the entrepreneurial sector.

When it comes to the education system, during the last few years, vocational training provision has been reformed and changes in the conditions for admission to advanced vocational training have been introduced.

Structure

Advanced vocational training is organised in training cycles , which have a modular structure. It includes a project vocational module during the last stage of the training cycle.

There are currently 89 advanced level qualifications (Source: todo FP). In addition, it is still possible to study five qualifications belonging to the now abrogated Organic Law 1/1990 on the General Organisation of the Education System [LOGSE] (Source: todo FP).

These training cycles belong to 25 of the 26 professional families established by the National Catalogue of Professional Qualifications (CNCP).

Aim and Objectives

The aim of vocational training in the education system is to qualify students for the activity in a professional field and to facilitate their adaptation to the changes in the labour market that may occur throughout their lives, as well as to contribute to their personal development and the exercise of democratic and peaceful citizenship, and to enable their progression in the education system, within the framework of lifelong learning.

The **objective** of advanced vocational training is to provide students with the professional, personal and social competences they will need in order to:

- Engage in a professional activity related to the general competence area of the relevant Vocational Training programme;
- Understand the organisation and characteristics of the relevant productive sector, the mechanisms for professional insertion, the pertinent labour legislation and the rights and obligations arising from labour relationships;
- Consolidate the habits of discipline, individual and teamwork, as well as the ability for self-learning and for critical analysis;
- Establish interpersonal and social relationships, both at professional and personal levels, based on the peaceful resolution of conflicts, the respect to others and the rejection of violence or any kind of prejudice and sexist behaviour;
- Prevent labour and environmental risks, and implement measures to work under conditions of good health and safety;
- Develop a motivating professional identity for future learning, and be able to adapt to the evolution of production processes and to social changes;
- Promote creativity, innovation and entrepreneurship;
- Use information and communication technologies, as well as the foreign languages required in their professional activity;
- Communicate effectively both at professional and personal levels;
- Manage their professional careers, analysing the most suitable training itineraries in order to improve employability.

Structure of the Academic Year

Activity in schools starts on September 1st and ends at least on June 30th. For students the teaching activity begins during the month of September and ends depending on the duration in hours of each training cycle. In any case, the total number of hours required in each case must be guaranteed.

The exact dates are set by the education authorities in each autonomous community, with different timings. The teaching activity is organised taking into account the Christmas, Easter and summer holidays, giving rise to terms of varying length. However, some Autonomous Communities have also tried to divide the year in two month periods.

During the summer holidays, educational institutions may remain open until the end of July **for administrative purposes**. Depending on the organisation of each educational centre, the same may occur on non-holiday days during the Christmas and Easter breaks.

Institutions Providing Advanced Vocational Training

VT studies can be pursued in vocational training institutions, integrated institutions or national reference institutions, which are specialised in the different productive sectors.

EducationPpolicy for Advanced Vocational Training

The **priority objectives** of the Spanish educational policy regarding advanced vocational training focus on several aspects:

- The incorporation of the following approaches that are key to adapting the education system to present needs:
    - Gender equality through co-education and the promotion of effective equality between women and men, the prevention of gender violence and respect for affective-sexual diversity;
    - A cross-cutting approach aimed at ensuring that all students have guarantees of success in education through a dynamic of continuous improvement of educational institutions and a greater individualisation of learning;
    - Focus on sustainable development in line with the 2030 Agenda;
    - The digital transformation taking place in all societies and which inevitably affects educational;
- Several strategic objectives:
    - Promoting lifelong learning and teacher mobility;
    - Improve the quality of the educational provision;
    - Guaranteeing educational inclusion and quality education for all students;
    - Guaranteeing equal opportunities in the fulfilment of the right to education;
    - Encouraging participation in education;
    - Promoting professional development;
    - Promoting the learning of foreign languages.

Specialised Education

Specialised education that composes higher education includes several advanced artistic programmes (specifically, professional plastic arts and design studies, and advanced artistic studies) and advanced sports education.

Artistic Education: Advanced Professional Studies in Plastic Arts and Design

Structure

Advanced vocational education in Plastic Arts and Design comprises the set of training actions that enable the qualified performance of the various professions related to the field of design, applied arts and artistic crafts, access to employment and active participation in social, cultural and economic life, as well as the updating and development of professional and personal skills throughout life.

These programmes are structured in advanced training cycles, grouped into professional families, with a module-based organisation and practical training periods in companies, studios and workshops.

Additionally, they include a module which requires the preparation of a project during the last stage of the training cycle.

There are currently 50 training cycles on offer, belonging to one of the 13 existing artistic professional families (Source: educagob).

Students passing the advanced level of plastic arts and design are awarded the diploma of Plastic Arts and Design Technician in the corresponding speciality, belonging to level 1 of the MECES.

Aim and Objectives

The **purpose** of advanced plastic arts and design professional studies is to:

- Provide the appropriate artistic, technical and technological training for the qualified exercise of the professional competences for each degree;
- Provide information on the organisational, economic, legal and safety aspects that affect professional practice, labour relations and the business environment of the corresponding professional sector;
- Enable students to gain access to employment, either as self-employed or wage-earning professionals, and foster entrepreneurship and lifelong learning.

The **aim** of these courses is to enable students to:

- Develop the skills associated with each degree and begin professional practice with guarantees of quality, efficiency and profitability;
- Value the importance of the plastic arts as a universal creative language and as a means of cultural expression, as well as the enrichment that traditional and modern artistic crafts and procedures represent for them;
- Encourage the renewal of the arts and cultural industries through aesthetic reflection and mastery of artistic production processes;
- Develop the potential for entrepreneurship, self-learning and adaptation to the evolution of artistic conceptions and technical processes, and use the channels of information and continuous training related to the exercise of their profession and the pursuit of personal and professional initiatives;
- Understand the organisation and characteristics of their professional environment, the legal aspects affecting labour relations in the relevant professional sector, as well as the basic and specific mechanisms for integration in the labour market;

- Develop skills and abilities in the priority areas defined within the guidelines established by the European Union, especially those relating to information and communication technologies, languages, teamwork and the prevention of occupational risks.

Likewise, professional plastic arts and design studies must promote effective equality of opportunities among people, regardless of their origin, race, sex, disability and other personal or social circumstances, for access to education and professional practice.

Structure of the Academic Year

As these programmes are structured in advanced training cycles, similar to those of vocational training, the organisation of the academic year is similar to the one set out in these programmes, although each degree may have its own specifications.

Institutions Providing Specialised Education

Advanced professional plastic arts and design studies are provided at art schools (public centres) and at authorised art schools (private centres).

Artistic Education: Advanced Artistic Education

Structure

Artistic Education is the set of programmes in the education system that aim to provide quality artistic training and guarantee the qualification of future professionals in music, dance, drama, plastic arts and design.

Advanced Music and Dance education, Dramatic Arts education, Preservation and Restoration of Cultural Assets education, advanced Design studies and advanced Plastic Arts studies, including advanced studies of Glass and Ceramics, have the status of Advanced Artistic Education.

The degrees in Advanced Degrees in Artistic Education that correspond to level 2 (Degree) of the MECES have the following denomination, followed by the speciality:

- Higher Degree in Conservation and Restoration of Cultural Heritage;
- Higher Degree in Design;
- Higher Degree in Plastic Arts;
- Higher Degree in Ceramics;
- Higher Degree in Glass.

The degrees in Advanced Degrees in Artistic Education that correspond to level 3 (Master) of the MECES have the following denomination, followed by the speciality:

- Higher Degree in Music;
- Higher Degree in Dance;
- Higher Degree in Performing Arts.

The designation of Master's degrees is Master in Artistic Education, followed by the specific name of the degree.

Aim and Objectives

The **purpose** of these degrees in advanced artistic education is to provide general training, in one or more disciplines, aimed at preparing students for the exercise of professional activities.

The aim of the official Master's artistic education is for each student to acquire advanced training, of a specialised or multidisciplinary nature, aimed at academic or professional specialisation, or at promoting initiation into research tasks.

Structure of the Academic Year

As it is equivalent to university education, the organisation of the academic year is similar to that of universities, although each degree may have its own specifications.

Institutions Providing Specialised Education

Advanced studies in music and dance are taught in conservatories or higher schools of music and dance and performing arts programmes in higher drama schools; conservation and restoration of cultural assets is taught in higher schools of conservation and restoration of cultural assets; advanced studies in plastic arts are taught in higher schools for the corresponding speciality and advanced studies in design are taught in higher design schools.

Advanced Sports Education

Structure

Sports education is organised on the basis of the sports modalities and, where appropriate, their specialisations, recognised by the Superior Sports Council (CSD), in accordance with Article 14.f of Law 39/2022 on Sports.

The programmes are structured in advanced training cycles, grouped into professional families, with an organisation in blocks and modules of variable duration, made up of areas of theoretical and practical knowledge appropriate to each professional and sports field.

Additionally, they include a module which requires the preparation of a final project during the last stage of the training cycle.

There are currently 18 training cycles on offer, belonging to 12 of the 14 existing sports professional families(Source: CSD).

Students successfully passing advanced sports education programmes will be awarded the Sports Technician diploma in the corresponding modality.

Aim and Objectives

The **purpose** of sports education is to prepare students for their professional activity in the sports system in relation to a sport modality or speciality, as well as to facilitate their adaptation to the evolution of the working and sports world and to active citizenship.

The **aim** of these courses is to enable students to:

- Develop the general skills corresponding to the professional profile defined in the corresponding degree;
- Guarantee the professional qualification in initiation, guidance, basic training, technical improvement, and single and team training for high-performance athletes in the corresponding modality or speciality within the sports system;
- Understand the characteristics and organization of the respective modality or speciality and of the sports system and know the rights and obligations arising from their functions;

- Acquire the knowledge and skills necessary to carry out their work under safe conditions, improving the quality and safety of the sports environment and taking care of the environment and people's health, and also facilitate the integration and normalisation of people with disabilities in the practice of sports;
- Develop a motivating professional identity and maturity for future learning (life-long learning, permanent training) and adaptations to changes in the initiation and improvement of the sports modality and in high-performance sport;
- Develop and convey the importance of individual responsibility and personal effort in sports practice and teaching;
- Develop and convey the ethical values linked to fair play, respect for others, the healthy practice of sports and the respect and care of one's own body;
- Enable the fulfilment of business activities and initiatives.

Likewise, sports education should promote equal opportunities for men and women, as well as for people with disabilities.

Structure of the Academic Year

As these programmes are structured in advanced training cycles, similar to those of vocational training, the organisation of the academic year is similar to the one set out in these programmes, although each degree may have its own specifications.

Institutions Providing Specialised Education

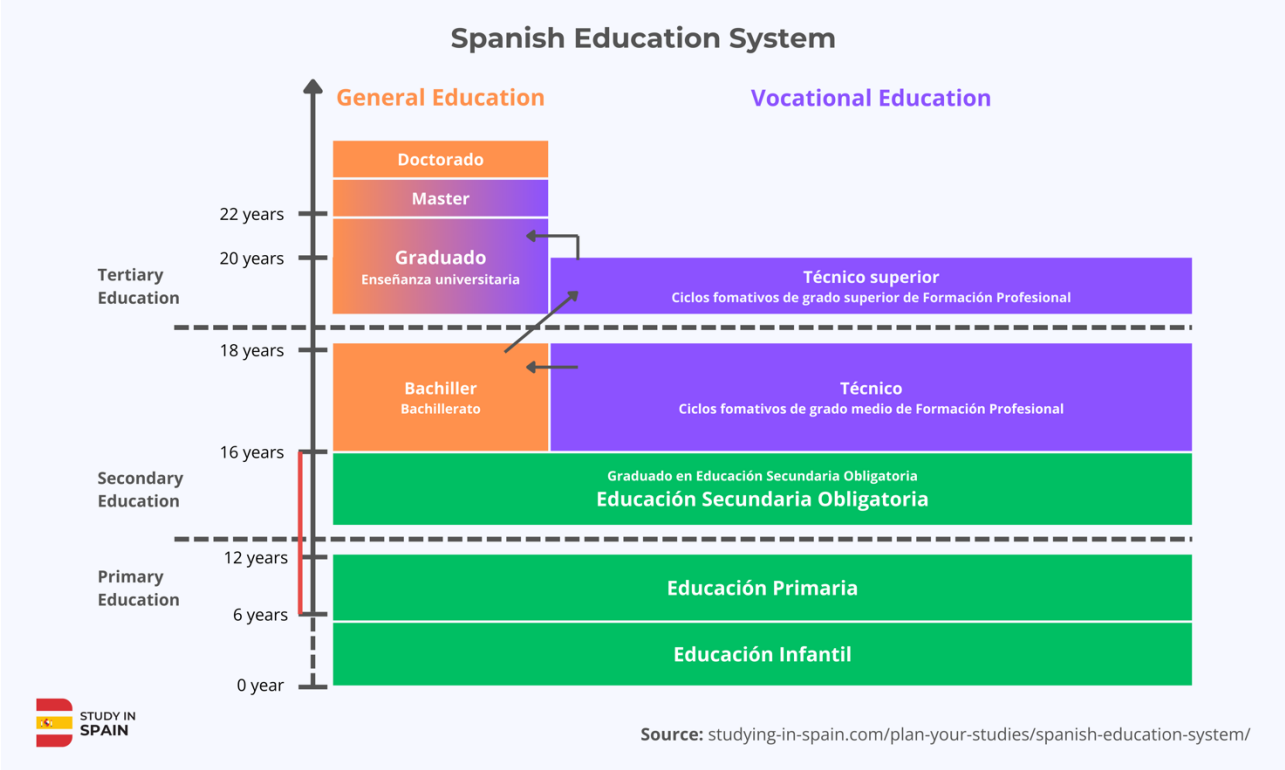
Advanced sports education is provided in public or private training centres authorised by the corresponding education authorities; integrated vocational training centres; national reference centres specialised in the sports sector or teaching centres within the military education system.
Exceptionally, the education authorities may authorise centres promoted by Spanish sports federations for the specific block of certain cycles of sports education.

Education Policy in Specialised Education

The **priority objectives** of the Spanish educational policy regarding specialised education focus on several aspects:

- The incorporation of the following approaches that are key to adapting the education system to present needs:
    - Gender equality through co-education and the promotion of effective equality between women and men, the prevention of gender violence and respect for affective-sexual diversity;
    - A cross-cutting approach aimed at ensuring that all students have guarantees of success in education through a dynamic of continuous improvement of educational institutions and a greater individualisation of learning;
    - Focus on sustainable development in line with the 2030 Agenda;
    - The digital transformation taking place in all societies and which inevitably affects educational;
- Several strategic objectives:
    - Promoting lifelong learning and teacher mobility;
    - Improve the quality of the educational provision;

- Guaranteeing educational inclusion and quality education for all students;
- Guaranteeing equal opportunities in the fulfilment of the right to education;
- Encouraging participation in education;
- Promoting professional development;
- Promoting the learning of foreign languages.



F. CZECHIA

The tertiary education sector is divided into higher education (ISCED 645, 7, and 8) and tertiary professional education (ISCED 655). The term tertiary education is not defined in the present legislation but is used in official documents. Higher education and tertiary professional education applicants qualify for entry if they have completed secondary education with a *Maturita* examination (*maturitní zkouška*, ISCED 344 or 354) and meet the admission requirements stipulated by a relevant institution.

Higher Education Institutions

Higher education is realised at higher education institutions (*vysoké školy*), which form the highest level of the Czech education system. Higher education consists of three types of degree programmes:

- **Bachelor's degree programme (ISCED 645)**, lasting 3–4 years
- **Master's degree programme** (ISCED 7), lasting 1–3 years **(ISCED 747)**, or 4–6 years in the case of programmes not following bachelor's programmes – non-structured study programme **(ISCED 746)**
- **Doctoral degree programme (ISCED 844)** lasting 3–4 years

Higher education institutions are **public, state, and private**. Under the Higher Education Act, they are classified as either **university type** (24 public, 2 state, and 3 private) which offer study programmes at all three levels linked with scholarly, research, developmental, artistic and other creative activities, or **non-university type** (2 public and 23 private) which mainly offer Bachelor's programmes but may also provide Master's programmes. (*Source: Ministry of Education, Youth and Sports*)

Completed secondary education with a *Maturita* examination is the basic **prerequisite for entry** into Bachelor's and non-structured Master's programmes. Detailed admission requirements are set by a relevant higher education institution and usually include an entrance examination. Higher education can take **forms** of on-site courses, distance learning courses or a combination of both.

Students have to follow a study plan within an accredited degree programme; **accreditation** is awarded by the National Accreditation Bureau for Higher Education (Accreditation Bureau). Accreditation is either institutional, which means that the higher education institution obtains the right to approve and manage its study programmes in the accredited areas of education, or each study programme is accredited by the Accreditation Bureau. The Education Act sets 37 educational areas. Within one educational area, the programmes of close or similar specialisation as to its content are prepared, approved and implemented, reflecting the common theoretical and methodological basis of the given area. Each study programme is assigned to one or more educational areas (the latter is a combined study programme). Creation and provision of study programmes is one of the recognised academic rights and freedoms of higher education institutions, so their number and prevailing orientation changes in time.

Studies are duly completed if students obtain their qualification through:

- A Bachelor's degree programme which ends with the final state examination (*státní závěrečná zkouška*), part of which is usually the defence of a thesis, graduates are awarded the academic title Bachelor (Bc.) or Bachelor of Arts (BcA.) in the field of art;

- A Master's degree programme which ends with the final state examination, part of which is the defence of a thesis, graduates mostly obtain the academic title Master (Mgr.) or Engineer (Ing.). Graduates who gained a Master's degree (academic title Mgr.) obtain another academic title if they fulfil additional advanced study examination (*rigorózní zkouška*) in the same study area;
- A Doctoral degree programme which ends with the state doctoral examination (*státní doktorská zkouška*), part of which is the defence of a thesis, graduates mostly obtain the academic title Doctor (Ph.D.).

As of 31 December 2022, the overall number of higher education students was more than 304 thousand. There were 184 thousand of students (60 %) in Bachelor's degree programmes, 69 thousand (23 %) in the follow-up Master's degree programmes, 33 thousand (11 %) in Long-cycle Master's degree programmes and more than 20 thousand (7 %) in Doctoral degree programmes (on-site courses, distance learning courses or a combination of both is the basis for calculating the number of students). The sum of the number of Bachelor's, Master's, Long-cycle Master's, and Doctoral degree students is higher than the total number of head counts. This is caused by the fact that some students are enrolled in several degree programmes. *(Source: Ministry of Education, Youth and Sports.)*

Tertiary Professional Schools

Tertiary professional education (ISCED 655) is provided at tertiary professional schools (*vyšší odborné školy*). Tertiary professional schools are **public, state, private or denominational**. They are regulated by the Education Act.

Upper secondary education with a *Maturita* examination is the **prerequisite for admission**. Admission procedure details are set by the school head and can include an entrance examination. The courses usually include both a theoretical and a practical part. They can take a form of day form, evening, distance, or combined studies The number of students in a **study group** is between 10 and 40 students. Educational programme is subject to **accreditation** from the Ministry of Education, Youth and Sports that is awarded on the basis of a recommendation of the Accreditation Commission for Tertiary Professional Education.

Education ends with a **graduate examination** (*absolutorium*), an examination consisting of a theoretical part in vocational subjects, an exam in a foreign language and a defence of a thesis. Graduates obtain graduate examination certificates, a diploma and the title "specialist with a diploma" (DiS.).

School-leavers from tertiary professional education **do not have access to Master's degree programmes (following Bachelor's programmes)**. Some higher education institutions, however, offer the possibility to acknowledge the subjects studied within a tertiary professional school programme and thus enabling the school-leavers to complete a Bachelor's degree programme in a shorter period of time.

Tertiary professional education in conservatoire (ISCED 554) is acquired through successful completion of a six-year or eight-year educational programme. The studies proceed continuously involving also secondary level of education. Pupils can also receive upper secondary education with a *Maturita* examination (ISCED 354).

Compared to the higher education, the above education has significantly fewer students. In the school year 2022/23, more than 20 thousand of students studied at tertiary professional schools, and less than 4 thousand of students at conservatories. 151 tertiary professional schools and 18 conservatoires operated in this school year. *(Source: Ministry of Education, Youth and Sports*.
Individual types of higher education programmes are described in following parts: Bachelor's Degree Programmes, Second Cycle Programmes (Master's degree programmes), Master' s non-structured study programmes and Third Cycle (PhD) Programmes (Doctoral degree programmes).
Education at tertiary professional schools is described in Chapter 7 on Tertiary professional schools, education at conservatoires due to the nature of the study in Chapter 6 on Upper Secondary and Post-Secondary Non-Tertiary Education.
Administration and governance of tertiary education at national, regional, local and institutional level is provided separately in Chapter 2 on Organisation and Governance. Section Organisation of Private Education of Chapter 2 deals with information on private higher education institutions and tertiary professional schools.

General Objectives

Higher Education Institutions
Higher education institutions (*vysoké školy*) are supreme centres of education, independent knowledge and creative activity. The general goal of higher education is to provide students with adequate professional qualifications, prepare them for engagement in research and participating in lifelong learning, make them contribute to the development of civic society and international, particularly European cooperation. They attain this goal by linking instruction with scholarly, research, developmental, artistic and other creative activities.
The Higher Education Act obliges the Ministry of Education, Youth and Sports to issue, annually update and publish the Strategic Plan of the Ministry. Currently valid document is the Strategic Plan of the Ministry for Higher Education for the Period from 2021. The priority goals of the higher education policy are the following:

- Develop competencies directly relevant to life and practice in the 21st century.
- Improve the availability and relevance of flexible forms of education.
- Improve the efficiency and quality of doctoral studies.
- Strengthen strategic management and the effective use of capacities in research and development at higher education institutions.
- Build capacity for the strategic management of higher education.
- Reduce the administrative burden on the staff of higher education institutions so that they can fully pursue their mission.

Tertiary Professional Schools
Tertiary professional education (*vyšší odborná škola*) develops and promotes knowledge and skills students acquired in secondary education and provides general education and vocational training for them to perform demanding professional activities. It is understood to be professional training.
In line with the Education Act, the Ministry of Education, Youth and Sports issues the Long-term Plan for Education and the Development of the Education System of the Czech Republic. The long-term plan sets plans, goals and criteria for the education policy at the education levels from the pre-

primary up to the tertiary professional level. For the period 2023-2027, it is based on the Long-Term Plan for Education and the Development of the Education System of the Czech Republic (2019-2023) and is aimed mainly at personal development and motivation for lifelong learning, ensuring modern education and preparation of teachers, and creating sustainable and effective system based on responsibility for education outcomes. In 2020 the government approved the Strategy for Education Policy of the Czech Republic 2030+. It is aimed at acquiring competencies for active life and equal opportunities in education. The content of the Strategy 2030+ is based on the partial goals and measures of the long-term plan for the period 2019-2023. The main tasks for the area of tertiary professional education in the period 2019–2023 were:

- To innovate in the new accredited higher education programmes with regard to the changing labour market
- To widen the range of higher vocational education programmes and continue the professional discussion leading to better permeability between tertiary professional education and higher education
- To link the process of accreditation of the tertiary professional education programme with entry in the School Register

See also Current strategies in the area of education in Chapter 2.

Legislative Framework

Tertiary education field is regulated by two laws:

- Higher Education Act
- Education Act, which regulates tertiary professional education in one part and in another one regulates education in conservatoires.

Higher Education Institutions

The **Higher Education Act** of 1998 (with more than thirty amendments) sets forth the mission of higher education institutions (*vysoké školy*), the academic community and academic freedom. It defines the position of public, state and private higher education institutions, their bodies or structure; for public schools it sets out rules for asset management. It establishes basic framework for the funding of higher education institutions, describes conditions under which an institution applying for the status of a private higher education institution can gain state approval, regulates the relationship between higher education institutions and the Ministry of Education, Youth and Sports, mentions the body representing higher education institutions and and describes the information systems of higher education institutions.

It further:

- Describes the types of study programmes, rules and bodies for their accreditation,
- Regulates admission to a study programme, its course and completion, sets out the rules and duties for students and the policy for awarding academic titles,
- Regulates the position of academic staff,
- Regulates recognition of qualifications and their parts acquired abroad.

In a supplement to this Act, public and state higher education institutions are listed in detail as well as educational areas for which the higher education institution can acquire an institutional accreditation. Since 2019, the Act regulates the working hours of academic staff, specifies the activities that the academic staff member must perform (i.e. direct educational activities and

activities related, and scientific, research and development activities), and the place where these activities are carried out.

During 2020 the activities of higher education institutions were affected by the Covid-19 pandemic. This was taken into account by Act No. 188/2020 Coll., which set special rules concerning studies at higher education institutions and the activities of higher education authorities for the calendar year 2020. For example, the law reflects restrictions on study programmes during the pandemic, their impact on admission procedures, graduation, including hybrid and distance forms, or on the course of study and the academic year schedule. The impact of the pandemic was also manifested in the following year, when the amendment to the Higher Education Act No. 495/2020 came into force in January 2021. Sections of the law describe what the higher education institution is entitled to in emergency situations. The experience with distance learning from the pandemic period resulted also in the publication of a methodological guideline by the National Accreditation Bureaufor the use of distance learning elements in onsite studies.

Activities of higher education institutions are also governed by their **internal regulations** that follow on from the Higher Education Act and are **subject of registration** to the Ministry of Education, Youth and Sports. For each higher education institution, ten internal regulations are mandatory and further regulations may be required by the school's statutes.

Some aspects of higher education are regulated in more detail by implementing rules:

- Government Regulation on the Accreditation Standards in Higher Education
- Government Regulation on the Educational Areas in Higher Education
- Decree on Procedure and Conditions of Publication of Results of Admission Procedure at Higher Education Institutions
- Decree on Submitting Data to the Register for Managing the Applications for Recognition of Foreign Higher Education and Qualifications
- Decree on Submitting Data to the Registry of Associate Professors, Professors and Distinguished Professors
- Decree on Submitting Statistical Data by Higher Education Institutions

Tertiary Professional Schools

The **Education Act** defines the goal and the level of tertiary professional education, its organisation and admission requirements, course and completion of study programmes, attained qualification and the manner in which accreditation of study programmes is granted. The amendment of 2020 introduced the obligation of schools to provide education to students in a distance form, the obligation of students to participate in this education respectively.

Further particulars about types of tertiary professional schools (*vyšší odborné školy*), organisation of study, course of study and its completion, tuition and accreditation of study programmes are specified by a Decree on Tertiary Professional Education. The system of education courses is governed by the Government Regulation on the System of Fields of Studies in Basic, Upper Secondary and Tertiary Professional Education.

Organisation of the School and Academic Year

Organisation of studies differs between tertiary professional schools (*vyšší odborné školy*) and higher education institutions (*vysoké školy*).

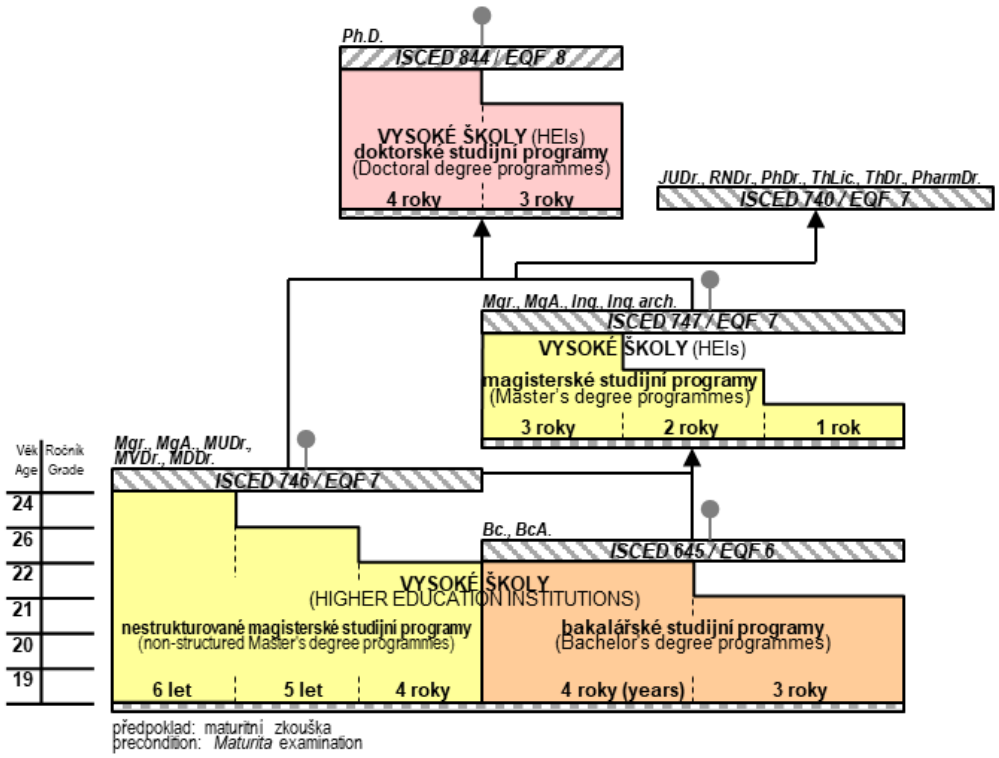
Higher Education Institutions

According to the Higher Education Act, the higher education can take forms of on-site courses, distance learning courses or a combination of both. The academic year lasts 12 months; the beginning is set by the Rector (*rektor*) usually for September or October. Studies are usually split into semesters, years or teaching blocks which cover periods of teaching activity, examinations and holidays. Most commonly, the academic year is split into semesters which have 14 weeks of teaching activity followed by a period of examinations. Summer holidays are in July and August, usually followed by an extended period of examinations. Details are stipulated in internal regulations of a relevant institution. For the year 2020 (incl. the winter semester of the academic year 2020/21), the Act No. 188/2020 Coll. took into account the effects of the Covid-19 epidemic and the academic year schedule.

Tertiary Professional Schools

According to the Education Act, the school year starts on 1 September and ends on 31 August covering the period of instruction and a summer holiday. The Decree on Tertiary Professional Education stipulates that the teaching activity period lasts 40 weeks (32 hours of instruction, 6 hours of self-study and assessment and 2 weeks of time reserve) and is split into a winter term (1 September to 31 January) and a summer term (1 February to 31 August). The last period of the educational programme instruction lasts at least 14 weeks. During a summer holiday, schools can offer compulsory courses, professional practice, or examinations, however, students should have at least 4 weeks of free time. Details on organisation of the school year are set by the school head in accordance with the accredited programme of study.

Schéma vysokoškolského vzdělávání v České republice v akademickém roce 2020/21
Diagram of the higher education in the Czech Republic 2020/21



Legenda (Explanatory notes):

přijímací řízení (admission procedure)

státní doktorská zkouška (doctoral state examination)

státní závěrečná zkouška (final state examination), státní rigorózní zkouška (advanced study examination)**

možnost další vzdělávací dráhy (possible progression routes)

pracovní trh (labour market)

* Existují dva typy státní rigorózní zkoušky: a) zkouška v medicínských oborech, b) zkouška, kterou lze složit bez dalšího studia po získání titulu magistr (Mgr.). (Two types of the advanced study examination exist: a) examination in medical fields, b) advanced study examination (without further study) after being awarded the Master's degree (magistr – Mgr.).)

Kódy ISCED odpovídají zařazení vzdělávacích programů, kódy EQF dosažené kvalifikaci. (ISCED codes relate to educational programmes, EQF codes to qualification attainment.)

Zdroj: Dům zahraniční spolupráce, Ministerstvo školství mládeže a tělovýchovy (Source: Czech National Agency for International Education , Ministry of Education, Youth and Sports

G. ITALY

This chapter describes the segment of the Italian education and training system that follows the completion of upper secondary education and that covers a set of different higher education systems:

- The higher university education, that includes universities and other equivalent institutions (*Formazione superiore di tipo Universitario ed equivalente*),
- The Higher education for the fine arts, music, and dance (*Alta formazione artistica, musicale e coreutica* - AFAM),
- The Higher technological tertiary education (*Sistema terziario di istruzione tecnologica superiore – ITS Academy*).

Universities are the primary seat of free research and free education within the framework of their respective regulations and are a place of learning and critical elaboration of knowledge; they operate, combining research and teaching in an organic manner, for the cultural, civil and economic progress of the country (legge 240/2010).

The institutes belonging to the higher university education system are:

- State universities and equivalent university institutes under special regulation,
- Non-State recognised universities,
- Private online universities,
- Higher schools for language mediators and specialisation institutes for psychotherapists.

AFAM institutions carry out production and research activities in the artistic field, in particular the fine arts, music, choreography, drama and design, in order to promote the achievement of educational objectives and the pursuit of high artistic and professional standards (DPR 212/2005).

The institutions belonging to the AFAM system are:

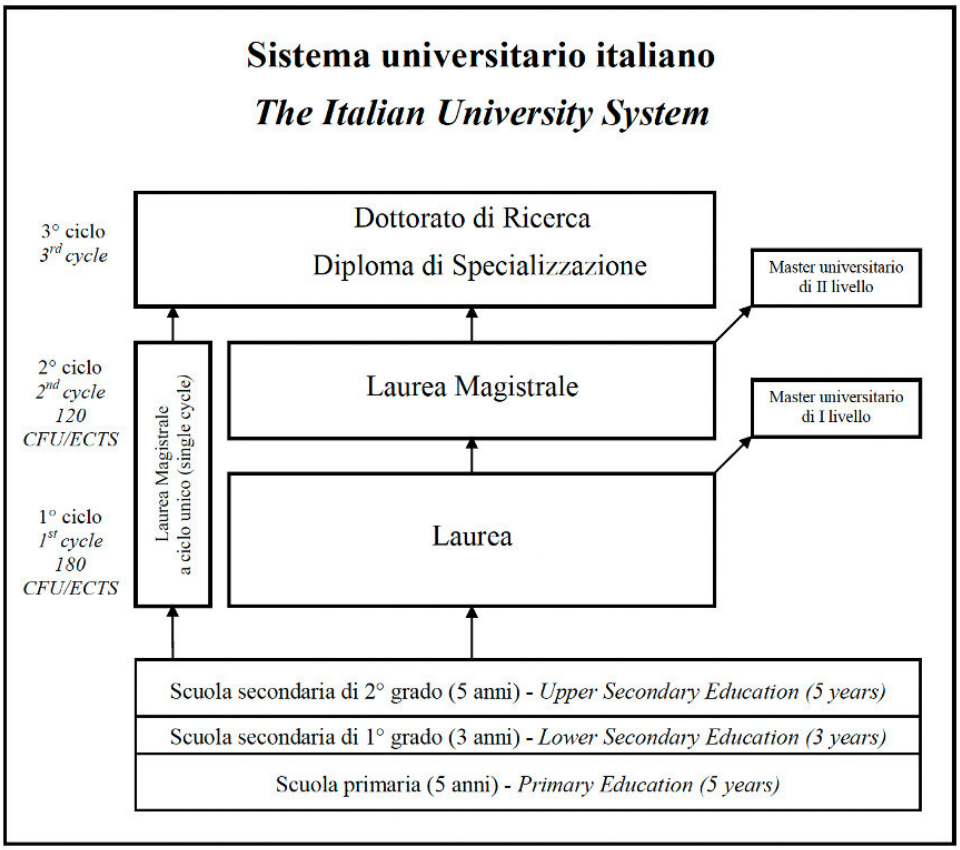
- State academies of fine arts (*Accademie di belle arti statali*),
- Recognised non-State academies of fine arts (*Accademie di belle arti non statali riconosciute*),
- Higher institutes for artistic industries (*Istituti superiori per le industrie artistiche* - ISIA)
- conservatoires (*Conservatori*),
- The National academy of drama (*Accademia nazionale d'arte drammatica*)
- The National dance academy (*Accademia nazionale di danza*),
- The officially recognised music institutes,
- Other institutions authorised to release recognised qualifications.

Institutions belonging to the higher university education and AFAM systems offer programmes and release qualifications of all the three levels of the Bologna process (Bachelor, Master, PhD), with a few exceptions. In addition, they may organise courses leading to other qualifications outside the Bologna structure. All the qualifications issued in the Italian education and training system, both State and Regional, are referenced to the NQF (pp. 85-89) that corresponds to the EQF. Qualifications issued by universities and AFAM institutions are also described in the Italian qualification framework of higher education (*Quadro dei titoli italiani dell'istruzione superiore* - QTI).

The providers of Higher technological education are the Higher technological institutes (*Istituti tecnologici superiori* - ITS Academies or ITSs) that are specialised tertiary institutions established to meet the demand of new and high-level competences coming from the labour world, of the technological sectors. ITSs have recently been reformed (law 99/2022).

Institutions of the university and AFAM systems as well as ITSs, have legal status and statutory, teaching, scientific, administrative, financial and accounting autonomy. They establish the organisation of the academic year, which, in general, starts on the 1st of October, ends on the 30th of September of the following year and is organised in semesters. For further details on the organisation of the academic year please refer to the Eurydice report '*The organisation of the academic year in Europe 2023-2024*'.

Besides universities, AFAM institutions and ITSs, other institutions offer courses leading to a qualification equivalent to a second-cycle qualification issued by universities (DM 87/2009). Among them: the Higher institute for the conservation and restoration (*Istituto superiore per la conservazione e il restauro*) in Rome, the School of the Gemstone Factory (*Scuola dell'Opificio delle pietre dure*) in Florence, with its branch in Ravenna at the School of Restoration of the Mosaic (*Scuola di restauro del mosaico*), the Higher school at the Central institute for the pathology of archives and books (*Istituto centrale per la patologia degli archivi e del libro*) in Rome. In general, access to courses requires an upper secondary education qualification and an entrance examination. The number of places available is limited and fixed annually. In some cases, also a previous relevant training is required. These institutes fall within the responsibility of the Ministry of culture instead of the Ministry of university and research and, therefore, their offer will not be described in this chapter.



I. LITUANIA

The Law on Higher Education and Research states that the mission of higher education and research is to help ensure the country's public, cultural and economic prosperity, provide support and impetus for the full life of every citizen of Lithuania, and satisfy the natural thirst for knowledge.

The studies provided by Lithuanian higher education institutions are conducted on the basis of study programmes conferring degree and non-degree study programmes. There are two types of study programmes: university and college study programmes. Studies can be of continual or extended forms. On completion of either form of studies, graduates obtain the corresponding education.

Since 1 January 2019, higher education studies have been broken down into four cycles:

1. Short cycle - the acquisition of a Lithuania qualification framework Level 5 qualification;
2. The first cycle - Professional Bachelor and Bachelor level;
3. The second cycle - Master's level;
4. The third cycle - Doctoral level.

Colleges together with VET schools can provide short-cycle studies. The first cycle Professional Bachelor study programmes may be delivered by colleges, whereas the first cycle Bachelor programmes are offered by universities. Study programmes conferring a second cycle degree may be conducted by universities. Doctoral studies may be delivered at universities or universities in conjunction with research institutes.

University degree conferring study programmes can be integrated, combining the first and second cycles of studies.

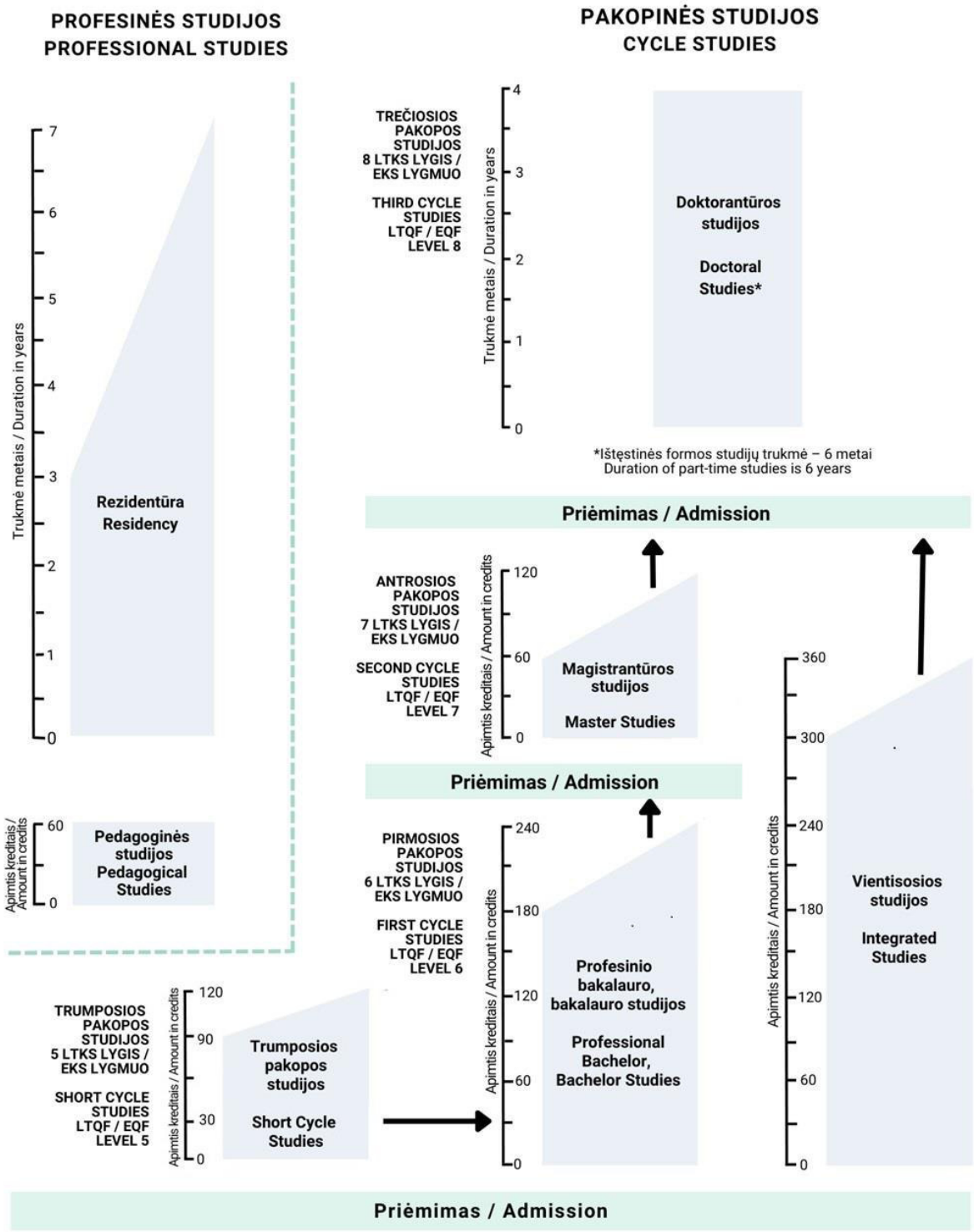
Study programmes aimed at retraining that do not award a degree, may be offered by universities and colleges in the manner prescribed by legal acts.

According to the Lithuanian Classification of Education, short-cycle studies belong to level 5. Bachelor studies (both university and non-university) belong to level 6, Master's studies to level 7, and Doctoral studies to level 8 (according to ISCED 2011).

The activities of the Lithuanian higher education system are regulated by the Law on Higher Education and Research(consolidated version of 01-03-2022).

A higher education institution may not organize studies in a field in which it has not been accredited. If there are students studying in such a field of studies, the Minister of Education, Science and Sports determines their further study opportunities. The studies of State higher education institutions must be assessed and accredited according to the needs of the State's economic, social and cultural development and the perspective of future development. The description of the procedure for external evaluation and accreditation of studies, the fields of assessment and indicators are approved by the Minister of Education, Science and Sports.

LIETUVOS AUKŠTOJO MOKSLO SISTEMA
LITHUANIAN HIGHER EDUCATION SYSTEM

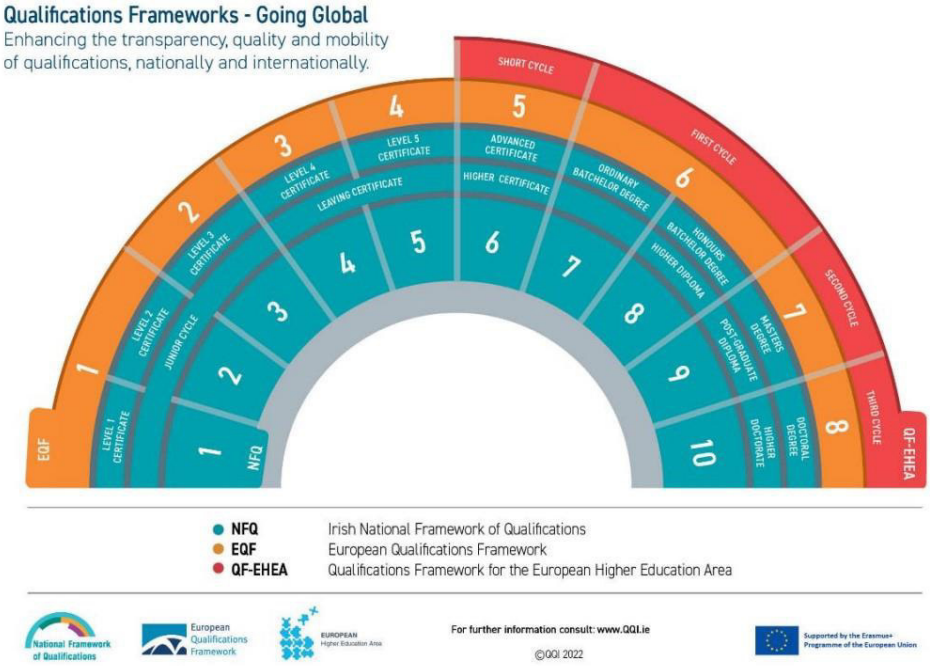


LTKS – Lietuvos kvalifikacijų sandara
LTQF – Lithuanian Qualifications Framework

EKS – Europos kvalifikacijų sandara
EQF – European Qualifications Framework

BOLOGNA FRAMEWORK/ EUROPEAN QUALIFICATIONS FRAMEWORK

The major awards of the NFQ are set out below together with the alignment to the 'Bologna Framework' and the alignment to the European Qualifications Framework (EQF):



EQF Level	EHEA Framework (Bologna)	National Framework	NFQ Major Award-Types
EQF Level 1		NFQ Level 1	Level 1 Certificate
		NFQ Level 2	Level 2 Certificate
EQF Level 2		NFQ Level 3	Level 3 Certificate;
EQF Level 3		NFQ Level 4	Level 4 Certificate; Leaving Certificate
EQF Level 4		NFQ Level 5	Level 5 Certificate; Leaving Certificate
EQF Level 5		NFQ Level 6	Advanced Certificate
	Short Cycle Higher Education		Higher Certificate
EQF Level 6	First Cycle Higher Education	NFQ Level 7	Ordinary Bachelor Degree
		NFQ Level 8	Honours Bachelor Degree; Higher Diploma
EQF Level 7	Second Cycle Higher Education	NFQ Level 9	Masters Degree; Post- Graduate Diploma
EQF Level 8	Third Cycle Higher Education	NFQ Level 10	Doctoral Degree; Higher Doctorate

Sample Evaluation Questionnaires

Project details: Joint Master's Degree Programme
in Cybersecurity Management & Data Sovereignty (Digital4Security)

Project ID: 101123430

Call: DIGITAL-2022-SKILLS-03

Table of Contents

Introduction

Digital4Security is a ground-breaking pan-European master's program aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. This €20m industry-led Master's, supported by funding from the DIGITAL Europe Programme, is a four-year initiative that comprises a Consortium of 36 partners spanning 12 countries. This master program will provide comprehensive knowledge of cybersecurity management, regulatory compliance, and technical expertise to European SMEs and companies.

Digital4Security is launching a collective cybersecurity revolution by harnessing the collective skill sets of our international Consortium, and the next generation of practical experts in the digital space. We're reskilling and upskilling graduates, professionals, managers and business leaders to become 'cyber confident', equipped to protect and empower European SMEs in the face of global cyber threats.

The Digital4Security curriculum is grounded in a rigorous needs analysis process involving all of our Consortium partners. The programme will blend academic and industry content to ensure graduates are equipped with both theoretical and job-ready cyber skills to fast-track employment. The program is designed to meet European accreditation standards and a wide range of national standards, with plans to offer micro-credentials for each module and industry certification in collaboration with our industry partners.

2. The Digital4Security Consortium

The Digital4Security Consortium is a dynamic pan-European partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management programme, developed and delivered by the best cybersecurity talent from Europe and worldwide. Table 1 lists the Higher Education Institutions (HEIs) jointly offering the master's degree, while Table 2 presents additional consortium partners, including industry stakeholders.

Table 1: Academic Partners (Higher Education Institutes) Offering the Joint Degree Program

No.	Partner	Abbreviation	Country
1	Universitatea Nationala de Stiinta si Technologies Politehnica Bucuresti	POLITEHNICA B.	Romania
2	National College of Ireland	NCI	Ireland
3	German University of Digital Science gGmbH	UDS	Germany
4	University of Rijeka	UNIRI	Croatia

5	Università degli Studi di Brescia	UNIBS	Italy
6	Politecnico di Milano	POLIMI	Italy
7	Universität Koblenz	UNI KO	Germany
8	CY Cergy Paris Université	CY	France
9	Mykolo Romerio Universitetas	MRU	Lithuania
10	Universidad Internacional de La Rioja	UNIR	Spain
11	Brno University of Technology	BUT	Czech Republic
12	Munster Technological University	MTU	Ireland
13	Vytautas Magnus University	VMU	Lithuania

Table 2: Associate Partners

No.	Associated Partner	Abbreviation	Country
14	DIGITAL TECHNOLOGY SKILLS LIMITED	DTSL	Ireland
15	IT@CORK ASSOCIATION LIMITED LBG	IT@CORK	Ireland
16	SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	SKILLNET	Ireland
17	ADECCO FORMAZIONE SRL	ADECCO TRAINING	Italy
18	ADECCO ITALIA HOLDING DI PARTECIPAZIONE E SERVIZI SPA	ADECCO GROUP	Italy
19	ADECCO ITALIA SPA	Adecco Italia	Italy
20	CEFRIEL SOCIETA CONSORTILE A RESPONSABILITA LIMITATA SOCIETA BENEFIT	CEFRIEL	Italy
21	ATAYA & PARTNERS	Ataya	Belgium
22	CYBER RANGES LTD	Cyber Ranges	Cyprus
23	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	FHG	Germany
24	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	NASK	Poland

25	POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	CMIP	Poland
26	SCHUMAN ASSOCIATES SCRL	SA	Belgium
27	CONTRADER SRL	Contrader	Italy
28	INDEPENDENT PICTURES LIMITED	indiepics	Ireland
29	MATRIX INTERNET APPLICATIONS LIMITED	MATRIX	Ireland
30	PROFIL KLETT D.O.O.	PROFIL KLETT	Croatia
31	SERVICENOW IRELAND LIMITED	ServiceNow	Ireland
32	EUROPEAN DIGITAL SME ALLIANCE	DIGITAL SME	Belgium
33	DIGITALEUROPE AISBL*	DIGITALEUROPE	Belgium
34	TERAWE TECHNOLOGIES LIMITED	TERAWE	Ireland
35	BANCO SANTANDER SA	BANCO SANTANDER /Santander	Spain
36	RED OPEN S.R.L.	RED OPEN S.R.L.	Italy

The HEIs, in conjunction with the Digital4Security consortium's industry partners, have collaborated and cooperated to jointly develop and design this programme and its curriculum.

Personal Feedback for Quality Management

In the context of a Joint Master's Degree in **Cybersecurity Management & Data Sovereignty**, following the European Approach to Quality Assurance, personal feedback is a cornerstone of our ongoing commitment to excellence. Continuous feedback from students, lecturers, and industry experts allows us to maintain the program's relevance, enhance teaching methods, and ensure the inclusion of cutting-edge cybersecurity trends and technologies. This iterative feedback loop supports not only the academic rigor of the program but also its alignment with evolving industry needs, contributing to the program's long-term success and accreditation.

This collection of sample questionnaires illustrates key areas of quality management, emphasizing the importance of regular feedback for monitoring and improvement. In particular, this document includes sample surveys for **students** (p. 7), focusing on areas such as:

- **Module Content**: Evaluating the clarity and relevance of course materials.
- **Teaching Effectiveness**: Assessing the delivery methods and engagement strategies used by instructors.
- **Learning Outcomes**: Gathering feedback on whether students feel equipped to meet the expected outcomes.
- **Inclusivity and Accessibility**: Understanding how well the program meets diverse learning needs.

All students will be invited to provide feedback on each module they completed during the previous semester. Lecturers use the module level feedback received from students to inform whether consideration should be given to explore alternative pedagogical strategies when delivering the module. The summarized outcomes of their module evaluations serve as the basis for improvement. Additionally, feedback regarding the overall learning platform will be collected less frequently, such as once during the first year and once in the final year of study.

Furthermore, surveys for **lecturers** (p. 18) serve to gather lecturers' reflections on their modules and the reception of their teaching by students. These surveys cover aspects such as:

- **Self-Assessment**: Encouraging instructors to evaluate their teaching methods and identify areas for improvement.
- **Student Engagement**: Gathering insights on student participation and enthusiasm for the course material.
- **Suggestions for Improvement**: Allowing educators to propose enhancements based on their experiences and feedback received.

Gathering teacher feedback facilitates quality management in several ways. First, comparing teacher and student feedback can reveal misperceptions, such as when a lecturer believes course materials are clear, but students provide significantly different responses.

Additionally, teacher feedback can be assessed by the Quality Enhancement and Curriculum Development Committee (QECDC, see Cooperation Agreement). This committee can identify common "pain points" across modules, aiding teachers in using the learning platform effectively and adopting best practices for student engagement.

Furthermore, continuous reflection on the grading process supports the Examinations Board and the Master's Board of Directors in guiding partners responsible for module delivery and grading. This approach helps refine assessment methods associated with learning outcomes, ensuring they are objective, reliable, valid, comprehensive, and feasible, thus promoting ongoing improvements in the examination process.

In addition, each module can undergo an annual evaluation by independent **industry experts** (p. 29), with at least two evaluators assigned per module. The sample surveys encompass:

- **Ensure Relevance to Industry Standards**: Assessing how well the module aligns with current industry practices and needs.
- **Content Quality**: Evaluating the depth and applicability of the subject matter.
- **Integration of Emerging Technologies**: Reviewing how effectively the module incorporates the latest advancements in cybersecurity.

By systematically collecting and analyzing this feedback, we are committed to fostering an environment of continuous improvement that enhances the educational experience for all stakeholders involved.

While the sample surveys included here highlight relevant areas and showcase potential assessment methods, the program's evaluation strategy remains flexible, capable of adapting its approaches and tracking additional parameters, such as drop-out rates and average grades, beyond those outlined in this document.

Sample Student Surveys

Demographic Information

1. **Age Group**
   - ☐ below 18
   - ☐ 18-24
   - ☐ 25-34
   - ☐ 35-44
   - ☐ 45-54
   - ☐ 55-64
   - ☐ 65 – 74
   - ☐ 75 – 84
   - ☐ 85 and above
   - ☐ Prefer not to say

2. **Gender**
   - ☐ Male
   - ☐ Female
   - ☐ Non-binary/Third gender
   - ☐ Prefer not to say

3. **Current Employment Status**
   - ☐ Employed full-time
   - ☐ Employed part-time
   - ☐ Self-employed
   - ☐ Unemployed
   - ☐ Student (not currently working)
   - ☐ Other (please specify)

---

4. **Level of Education**
   - ☐ High school diploma or equivalent
   - ☐ Associate degree

☐ Bachelor's degree

☐ Master's degree

☐ Doctorate

☐ Other (please specify)

Cybersecurity Background

1. **What is your current level of expertise in cybersecurity?**
   ☐ Novice (basic understanding of concepts)
   ☐ Intermediate (proficient in certain areas with practical experience)
   ☐ Advanced (highly skilled with extensive experience across multiple areas)
   ☐ Expert (recognized authority in the field)

2. **How many years of formal education or training do you have in IT, specifically focused on cybersecurity?**
   ☐ No formal training
   ☐ Less than 1 year
   ☐ 1-2 years
   ☐ 3-4 years
   ☐ 5 or more years

3. **How many years of practical experience do you have in the cybersecurity field (e.g., industry roles)?**
   ☐ No experience
   ☐ Less than 1 year
   ☐ 1-2 years
   ☐ 3-4 years
   ☐ 5 or more years

4. **In which areas of cybersecurity have you worked, if any?** (Select all that apply)
   ☐ Network Security (e.g., firewalls, intrusion detection systems)
   ☐ Information Security (e.g., data protection, encryption)
   ☐ Cyber Threat Intelligence (e.g., threat analysis, vulnerability assessments)

☐ Incident Response (e.g., crisis management, recovery planning)
☐ Penetration Testing (e.g., ethical hacking, security assessments)
☐ Compliance and Risk Management (e.g., GDPR, HIPAA)
☐ Cloud Security (e.g., securing cloud infrastructure, services)
☐ Other (please specify):

---

5. **Do you currently hold any certifications in cybersecurity?** (Select all that apply)
   ☐ CompTIA Security+
   ☐ Certified Information Systems Security Professional (CISSP)
   ☐ Certified Ethical Hacker (CEH)
   ☐ Certified Information Security Manager (CISM)
   ☐ Certified Information Systems Auditor (CISA)
   ☐ Other (please specify):

Module-Specific Feedback

Part 1 Content and Structure

1. **The module content was well-structured and easy to follow.**
   ☐ Strongly agree
   ☐ Agree
   ☐ Neutral
   ☐ Disagree
   ☐ Strongly disagree

2. **The balance between theoretical concepts and practical applications was appropriate.**
   ☐ Strongly agree
   ☐ Agree
   ☐ Neutral
   ☐ Disagree
   ☐ Strongly disagree

3. **The module was interactive, allowing for active participation and engagement.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

4. **The pace of the module was manageable for me.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

5. **The module topics were interesting and relevant to my academic or professional goals.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

Part 2: Workload

1. **Please think about your workload for this module. 1 ECTS credit should correspond to ca. 25 hours of work over the semester. Considering the ECTS points for this module, how much time did you actually spend?**
   - ☐ Much less than expected (significantly less than 25 hours per ECTS)
   - ☐ Somewhat less than expected
   - ☐ About the expected amount (around 25 hours per ECTS)
   - ☐ Somewhat more than expected
   - ☐ Much more than expected (significantly more than 25 hours per ECTS)

2. **If you found the workload to be significantly *less* than expected, what do you think were the reasons** *(choose all that apply)***?**
   - ☐ I was already skilled in the domain, so I completed tasks faster
   - ☐ The assignments or readings were shorter than anticipated

☐ The content was easier to understand than expected

☐ I had ample resources that made studying more efficient

☐ I completed some work alongside peers, which saved time

☐ Other reason:

---

3. **If you found the workload to be significantly *more* than expected, what do you think were the reasons** *(choose all that apply)***?**

   ☐ I did not understand key concepts and had to research them independently

   ☐ The assignments or readings were more extensive than anticipated

   ☐ I struggled with certain topics, requiring extra study time

   ☐ Instructions were unclear, and it took time to clarify tasks

   ☐ Technical issues slowed my progress

   ☐ Group work required additional coordination time

   ☐ Other reason:

Part 3 Practical Project & Interaction [only for modules with practical projects]

1. **The practical project was well-aligned with the theoretical parts of the module.**

   ☐ Strongly agree

   ☐ Agree

   ☐ Neutral

   ☐ Disagree

   ☐ Strongly disagree

2. **The course encouraged interaction between students (e.g., group work, discussions).**

   ☐ Strongly agree

   ☐ Agree

   ☐ Neutral

   ☐ Disagree

☐ Strongly disagree

3. **The level of interaction between students and the lecturer was sufficient.**
   ☐ Strongly agree
   ☐ Agree
   ☐ Neutral
   ☐ Disagree
   ☐ Strongly disagree

4. **The project provided ample opportunity for asking questions and receiving feedback from the lecturer.**
   ☐ Strongly agree
   ☐ Agree
   ☐ Neutral
   ☐ Disagree
   ☐ Strongly disagree

Part 4 Language and Communication

1. **I had no difficulty understanding the lecturer in English.**
   ☐ Strongly agree
   ☐ Agree
   ☐ Neutral
   ☐ Disagree
   ☐ Strongly disagree

2. **Communicating with fellow students during discussions was easy for me in terms of language usage (like English).**
   ☐ Strongly agree
   ☐ Agree
   ☐ Neutral
   ☐ Disagree
   ☐ Strongly disagree

3. **What languages did you use to interact with other students during the course?**
   ☐ English
   ☐ I primarily used English, but also other languages (please specify):

☐ I used other languages extensively (please specify):

4. **The course materials (e.g., slides, readings) were clear and understandable in English.**
   ☐ Strongly agree
   ☐ Agree
   ☐ Neutral
   ☐ Disagree
   ☐ Strongly disagree

Part 5 Inclusivity & Accessibility

1. The module provided a diverse range of media, including videos, texts, and talks, with options to toggle between visual and audio formats (e.g., high-quality subtitles for talks and text-to-speech functionality).
   ☐ Strongly agree
   ☐ Agree
   ☐ Neutral
   ☐ Disagree
   ☐ Strongly disagree

2. **The course content was accessible for individuals with hearing or visual impairments.**
   ☐ Strongly agree
   ☐ Agree
   ☐ Neutral
   ☐ Disagree
   ☐ Not applicable to me

3. **There were problems related to gender inequality during this course.**
   ☐ Strongly agree
   ☐ Agree
   ☐ Neutral
   ☐ Disagree
   ☐ Not applicable

   If you observed gender-related inequalities, please specify:

4. **There were problems related to ethnic inequalities during this course.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Not applicable

   If you observed ethnicity-related inequalities, please specify:

   _____

5. **Regarding accessibility and inclusivity, do you have any comments or suggestions for improving this module?**

   _____

Feedback on the Overall Online Study Platform

Part 1 Navigation & Usability

1. **The online study platform was easy to navigate.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

2. **Finding course materials, assignments, and announcements on the platform was straightforward.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

3. **The platform layout and design made it easy for me to track my progress across courses.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

4. **The platform's notifications (e.g., for deadlines or new content) were helpful and timely.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

Part 2 Online Learning Experience

1. **The online platform supported effective communication between students and teachers.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

1. **I found it easy to connect with fellow students for discussions or group work.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

2. **Participating in online sessions (lectures, webinars) felt engaging and interactive.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

3. **I experienced issues staying motivated in the online learning format.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

5. **The online learning format sometimes felt tiring compared to in-person learning.**
   - ☐ Strongly agree
   - ☐ Agree
   - ☐ Neutral
   - ☐ Disagree
   - ☐ Strongly disagree

6. **What advantages did you experience with online learning compared to face-to-face programs?**
   Please select all that apply:

   - ☐ Greater flexibility in scheduling
   - ☐ Ability to study from home
   - ☐ Opportunities to attend classes at varied hours
   - ☐ Compatibility with family commitments
   - ☐ Ability to work while studying
   - ☐ Access to a broader range of resources and materials
   - ☐ Increased comfort in a familiar environment
   - ☐ Reduced commuting time and costs
   - ☐ Environmental benefits due to fewer commutes
   - ☐ Lower tuition fees compared to traditional programs
   - ☐ Access to renowned instructors from across Europe
   - ☐ Other (please specify):

   _____

7. **What challenges or disadvantages did you encounter with online learning compared to face-to-face programs?**
   Please select all that apply:

   - ☐ Limited personal interaction with instructors

☐ Limited personal interaction with peers

☐ Difficulty maintaining motivation and focus

☐ Technical issues (e.g., connectivity problems, software difficulties)

☐ Challenges in managing time and balancing responsibilities

☐ Feelings of isolation or disconnection from the learning community

☐ Limited opportunities for hands-on experiences or practical application

☐ Difficulty in accessing course materials or resources

☐ Other (please specify):

_____

Sample Teacher Surveys

Lecturer Feedback Questionnaire

Part 1 General Module Feedback

1. **How would you rate the overall effectiveness of your module held in this semester?**
   ☐ Very effective
   ☐ Effective
   ☐ Moderately effective
   ☐ Ineffective

2. **If you have taught this module in previous semesters, did you notice any significant differences compared to earlier iterations?**
   ☐ This was the first time I held this module
   ☐ Certain aspects went better than before, specifically:
   If so, please describe:

   Possible reason(s):

   _____

   ☐ Some areas were more challenging than before, specifically:
   If yes, please describe:

   _____

   Possible reason(s):

   _____

3. **What do you think went particularly well in this module?**

   _____

4. **Which aspects of the module would you improve, and how?**

Part 2 Online Teaching Modality

1. **How would you evaluate the online learning platform (e.g., usability, stability, and functionality) for this module?**
   ☐ Excellent
   ☐ Good
   ☐ Fair
   ☐ Poor

2. **Did you encounter any technical issues during online teaching (e.g., platform crashes, poor video/audio quality)?**
   ☐ Yes
   ☐ No
   If yes, please describe the issues you faced:

---

3. **What platform functionalities were particularly helpful during the course?**

---

4. **How would you assess the effectiveness of online tools (e.g., breakout rooms, shared whiteboards, discussion forums) for supporting student engagement and learning?**
   ☐ Very effective
   ☐ Effective
   ☐ Moderately effective
   ☐ Ineffective

5. **Were you able to maintain interaction with students effectively in the online setting (e.g., discussions, Q&A sessions)?**
   ☐ Very effective interaction

☐ Mostly effective interaction
☐ Neutral
☐ Somewhat ineffective interaction
☐ Very ineffective interaction

6. **How tiring was online teaching for you compared to traditional face-to-face teaching?**
   ☐ Much more tiring
   ☐ Slightly more tiring
   ☐ The same
   ☐ Less tiring
   ☐ I never teach face-to-face, so I cannot tell

Part 3 Student Involvement and Inclusivity

1. **Were all students equally involved during the course (e.g., participation, assignments, discussions)?**
   ☐ Highly equal involvement
   ☐ Mostly equal involvement
   ☐ Neutral
   ☐ Somewhat unequal involvement
   ☐ Highly unequal involvement
   ☐ Unable to assess

2. **If there were differences in student participation, what do you believe contributed to these differences (e.g., time zones, technology access, motivation)?**

   _____

3. **Did you notice any issues of inclusivity related to students with disabilities (e.g., hearing or visual impairments)?**
   ☐ Yes
   ☐ No

   If yes, please describe:

   _____

4. **Did you observe any gender or cultural inequalities that affected participation or learning outcomes?**

   ☐ Yes

   ☐ No

   If yes, please describe:

   _____

5. **How did you address language barriers for students who may have faced challenges understanding the course content (lecturer's speech, slides, discussions, etc.)?**

   _____

Part 4 Learning Materials and Tools

1. **Did students report difficulties accessing or understanding the learning materials?**

   ☐ Yes

   ☐ No

   If yes, please describe:

   _____

2. **Were the digital tools (e.g., simulation software, cybersecurity labs) effective for delivering the practical aspects of the module?**

   ☐ Very effective

   ☐ Effective

   ☐ Moderately effective

   ☐ Ineffective

3. **If applicable, how could the integration of digital tools be improved in the module?**

Part 5 Practical vs. Theoretical Balance

1. **Did you find the chosen balance between theoretical content and practical exercises suitable for this module?**
   ☐ Perfectly suitable
   ☐ Mostly suitable, but a bit too much theoretical content
   ☐ Mostly suitable, but a bit too much practical content
   ☐ Too much theoretical content
   ☐ Too much practical content
   ☐ Not relevant to this module

2. **If not perfectly suitable, what in particular would you like to change (e.g., include or exclude)?**

---

3. **Did students show more interest in the theoretical content or practical exercises?**
   ☐ More active in theoretical content
   ☐ More active in practical exercises
   ☐ Equally active in both
   ☐ Engagement varied significantly among students

Part 6 Interaction and Support

1. **How interactive was the module?**
   ☐ Very interactive
   ☐ Moderately interactive
   ☐ Not particularly interactive

2. **How often did students reach out for support (e.g., clarification, feedback, technical issues)?**
   ☐ Frequently

☐ Occasionally

☐ Rarely

3. **If applicable, how could student-lecturer interaction be improved in the online setting?**

_____

Part 7 Assessment and Grading

1. **How straightforward did you find the assessment and grading process for this module?**

   ☐ Very straightforward

   ☐ Mostly straightforward

   ☐ Somewhat challenging

   ☐ Very challenging

   If you encountered challenges during the grading process, please specify:

   _____

2. **How much time did you personally spend on the assessment and grading process for this module over the semester?**

   ☐ Less than 1 hour

   ☐ 1-2 hours

   ☐ 2-4 hours

   ☐ 4-6 hours

   ☐ 6-8 hours

   ☐ More than 8 hours

3. **Did you involve any additional individuals in the assessment and grading process? If so, please specify their roles and the time they contributed.**

   _____

4. **Were the assessment criteria easy to apply?**
   ☐ Very clear and easy to apply
   ☐ Mostly clear, with some difficulties
   ☐ Somewhat unclear
   ☐ Very unclear

5. **Please share any suggestions you might have for improving the assessment and grading process?**

_____

Part 8 Final Remarks

1. **What aspects of the module do you like the most?**

_____

2. **What aspects of the module do you think require the most rework and improvement?**

_____

3. **How could alternative uses of digital tools on the learning platform, or improvements to the tools themselves, enhance the effectiveness of the module?**

_____

4. **How would you grade the module effectiveness on a scale from A (excellent) to F (fail)?**
   ☐A
   ☐B
   ☐C
   ☐D
   ☐F

5. **Are there any additional comments or suggestions you would like to provide regarding the program or module development?**

Appropriateness of Assessment Tasks for Master's Level

1. **To what extent do you believe the module's assessment tasks are appropriate for the qualification level of your students (i.e., master's level)? Were the tasks suitably difficult, too easy, or too challenging?**

   ☐ 1 (Far too easy, more suited for high school)
   ☐ 2 (Slightly too easy; better suited for bachelor's level)
   ☐ 3 (Appropriate for master's level)
   ☐ 4 (Slightly too challenging, approaching PhD level)
   ☐ 5 (Overly challenging, best suited for PhD level)

2. **Please describe any adjustments you believe are necessary to better align the assessment tasks with the appropriate qualification level for your students (i.e., master's level).**

Alignment of Assessment Tasks with Program Learning Outcomes

These are the overarching Program's Learning Outcomes.

Goal 1: Critically assess and evaluate cybersecurity principles, practices, and technologies relevant to modern enterprises.

Goal 2: Strategically apply cybersecurity knowledge and utilise practical skills and technologies for long-term success in cybersecurity leadership roles across diverse industries, government agencies, and institutional settings.

Goal 3: Identify knowledge gaps and undertake self-learning to acquire new knowledge to support professional development and the ability to adapt to evolving threats, technologies, and regulatory environments.

Goal 4: Exhibit and apply leadership skills necessary for effectively managing cybersecurity initiatives within organisations, including education and training, strategic planning, and resource allocation.

Goal 5: Critically evaluate and analyse cyber threats in order to implement effective security operations, and to enable the proactive identification, assessment, and mitigation of cyber threats.

Goal 6: Effectively apply analytical and strategic thinking in order to make decisions to address security requirements.

Goal 7: Communicate effectively across a range of complex and advanced cybersecurity concepts to provide leadership within an organisation and facilitate effective collaboration and teamwork.

Goal 8: Critically assess cybersecurity legal, information governance, and regulatory frameworks and practices to ensure effective oversight, auditing, risk mitigation, accountability, compliance, and strategic alignment with organisational objectives.

1. **Upon reflection, to what extent do you believe the module's assessment tasks adequately cover the relevant program learning outcomes?**
   ☐ 1 Significant gaps in alignment
   ☐ 2
   ☐ 3
   ☐ 4
   ☐ 5 Strong alignment with program learning outcomes

2. **Are there any program learning outcomes that should be addressed by your module, but are not sufficiently covered by the current assessment tasks? How could you modify your module and its assessments to improve this alignment?**

Objectivity of Grading Approach

1. **How would you rate the objectivity (fairness and impartiality) of your grading approach? For instance, would different assessors likely arrive at the same ranking of student performance, as an indication to grading objectivity in this module?**
   ☐ 1 Highly Subjective
   ☐ 2
   ☐ 3
   ☐ 4
   ☐ 5 Completely objective

Reliability of Grading Approach

1. **How consistent do you believe your grading is across different students and over time?**
   ☐ 1 Grading is inconsistent across students or over time
   ☐ 2
   ☐ 3
   ☐ 4
   ☐ 5 Grading is highly consistent across students and over time

Validity of Assessment Tasks

1. **How would you rate the validity of your assessment tasks (i.e., do they measure what they are intended to measure in relation to the module's learning outcomes)?**
   ☐ 1 Assessments do not adequately measure the intended learning outcomes
   ☐ 2
   ☐ 3
   ☐ 4
   ☐ 5 Assessments fully measure the intended learning outcomes

Qualitative Feedback on Objectivity, Reliability, and Validity

1. **What challenges have you encountered in ensuring objectivity, reliability, or validity in your assessments? How could your grading and assessment strategy be improved to address these challenges?**

Coverage of Module Content by Assessment Tasks

1. **To what extent do the assessment tasks and grading in the module comprehensively cover the key content areas?**
   ☐ 1 Major gaps in content coverage
   ☐ 2
   ☐ 3
   ☐ 4
   ☐ 5 Fully comprehensive coverage of key content

2. **Are there any significant areas of the module content that are not adequately addressed by the assessments? How might the assignments be adjusted to ensure that all key content is sufficiently assessed?**

Sample Surveys for Industry Experts

The sample questionnaire below is designed for experts who evaluate the module content based on full access to module descriptions and teaching materials, but who have not personally taken the class (as student feedback is gathered separately through dedicated surveys, see Sect. "Sample Student Surveys" above).

Part 1 Evaluator Information

1. **What is your current role in the cybersecurity field?**

   _____

2. **Which industry do you primarily work in?**

   _____

3. **How many years of experience do you have in cybersecurity within industries?**
   ☐ Less than 2 years
   ☐ 2–5 years
   ☐ 6–10 years
   ☐ More than 10 years

Part 2 Module Relevance to Industry Needs

1. **How relevant is the content of this module to current challenges and practices in your industry?**
   ☐ Extremely relevant
   ☐ Moderately relevant
   ☐ Slightly relevant
   ☐ Not relevant

2. **How relevant do you believe the content of this module is for industries in general?**
   ☐ Extremely relevant
   ☐ Moderately relevant

☐ Slightly relevant

☐ Not relevant

3. **How well does the module prepare learners for real-world cybersecurity scenarios in your specific industry?**

   ☐ Very well

   ☐ Adequately

   ☐ Poorly

   ☐ Not at all

4. **How well do you believe the module prepares learners for real-world cybersecurity scenarios in industries generally?**

   ☐ Very well

   ☐ Adequately

   ☐ Poorly

   ☐ Not at all

Part 3 Content Quality

1. **How would you rate the overall quality of the content presented in the module?**

   ☐ Excellent

   ☐ Good

   ☐ Average

   ☐ Poor

2. **How comprehensive is the coverage of relevant topics in the teaching area addressed by this module?**

   ☐ Very comprehensive

   ☐ Comprehensive, but some topics are missing

   ☐ Some relevant topics are covered, but many are missing

   ☐ Not comprehensive at all

3. **If you are missing subjects, please specify**

4. **How accurate do you find the information in this module?**

☐ Completely accurate
☐ Mostly accurate, but some areas need updates
☐ Some inaccuracies
☐ Frequent inaccuracies

5. **If you observe inaccuracies, please specify**

_____

6. **How clear and understandable is the material in this module for someone with your industry experience?**

☐ Very clear
☐ Clear, but some sections are complex
☐ Difficult to follow in parts
☐ Not clear at all

Part 4 Inclusion of Up-to-date Issues and Technologies

1. **How well does the module integrate emerging trends and technologies relevant across industries?**

☐ Excellent integration
☐ Sufficient integration
☐ Limited integration
☐ No integration

2. **Does the module address upcoming industry standards or regulations relevant across industries?**

☐ Yes, thoroughly
☐ Partially
☐ Not at all
☐ Not relevant in this module

3. **If there are trends or new topics you suggest for inclusion in this module, please specify:**

Part 5 Practical Applications

1. **Does the module include practical exercises or case studies that reflect challenges relevant in the industry?**
   ☐ Yes, extensively
   ☐ Somewhat
   ☐ No, or very little

2. **How useful are the hands-on components (e.g., labs, simulations) in preparing learners for tasks in the industry?**
   ☐ Extremely useful
   ☐ Moderately useful
   ☐ Slightly useful
   ☐ Not particularly useful

Part 6 Overall Assessment

1. **How would you rate the overall effectiveness of this module in preparing professionals for the specific areas of cybersecurity it aims to address?**
   ☐ Excellent
   ☐ Good
   ☐ Fair
   ☐ Poor

2. **How do you rate the overall industry relevance of this module?**
   ☐ Excellent
   ☐ Good
   ☐ Fair
   ☐ Poor

3. **Would you recommend this module to your colleagues?**
   ☐ Yes
   ☐ Maybe
   ☐ No

4. **Please name your reasons for (not) recommending the course:**

---

5. **What grade (A = best, F = fail) do you assign to this module?**

☐ A
☐ B
☐ C
☐ D
☐ E
☐ F

6. **Overall, what did you like most about this module?**

---

7. **Overall, what improvements would you suggest? Please share any ideas or wishes for enhancing the module.**
