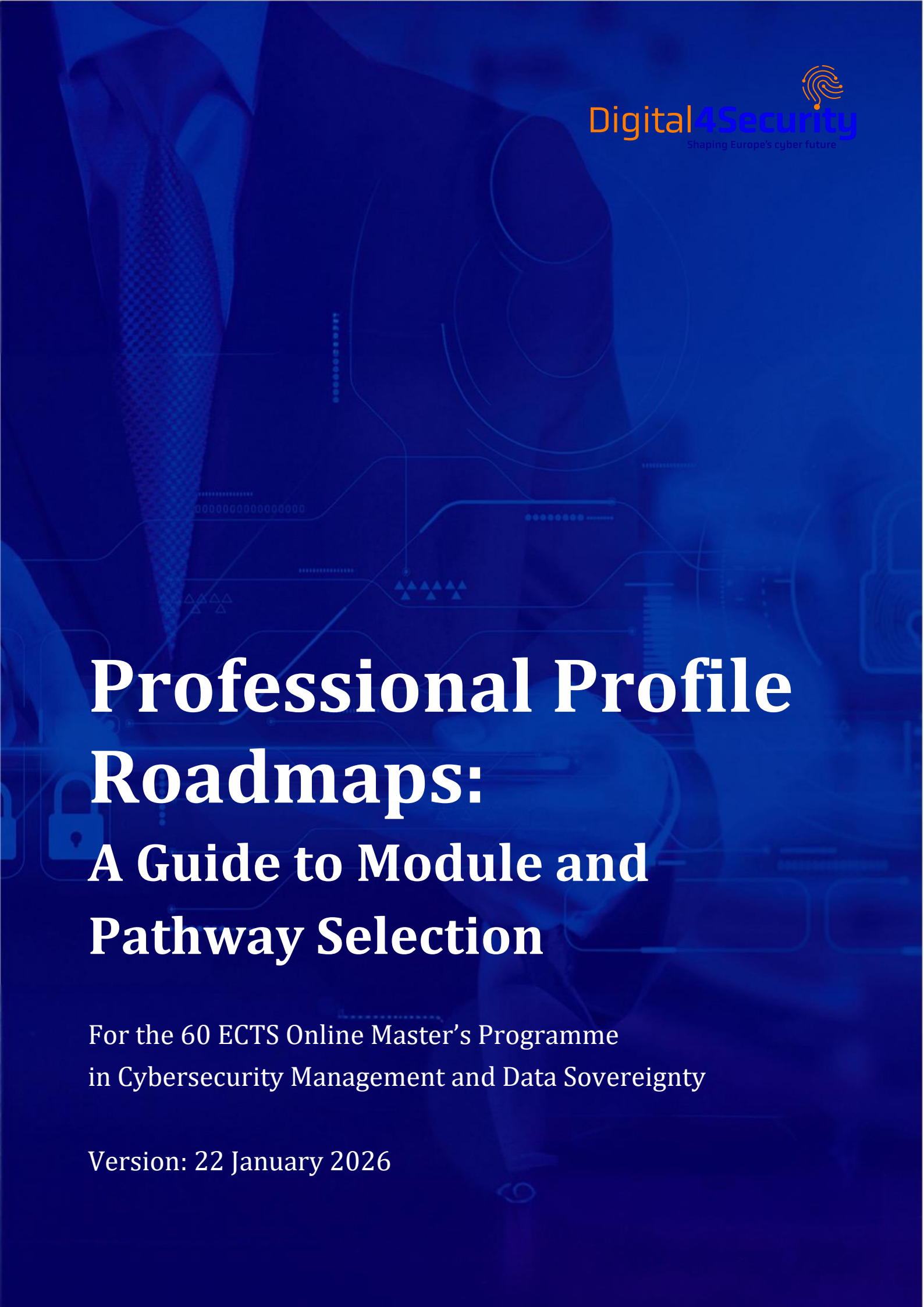


Digital4Security
Shaping Europe's cyber future

Professional Profile Roadmaps:

A Guide to Module and Pathway Selection

For the 60 ECTS Online Master's Programme
in Cybersecurity Management and Data Sovereignty

Version: 22 January 2026

Digital4Security
Shaping Europe's cyber future

Table of Contents

Introduction to Digital4Security

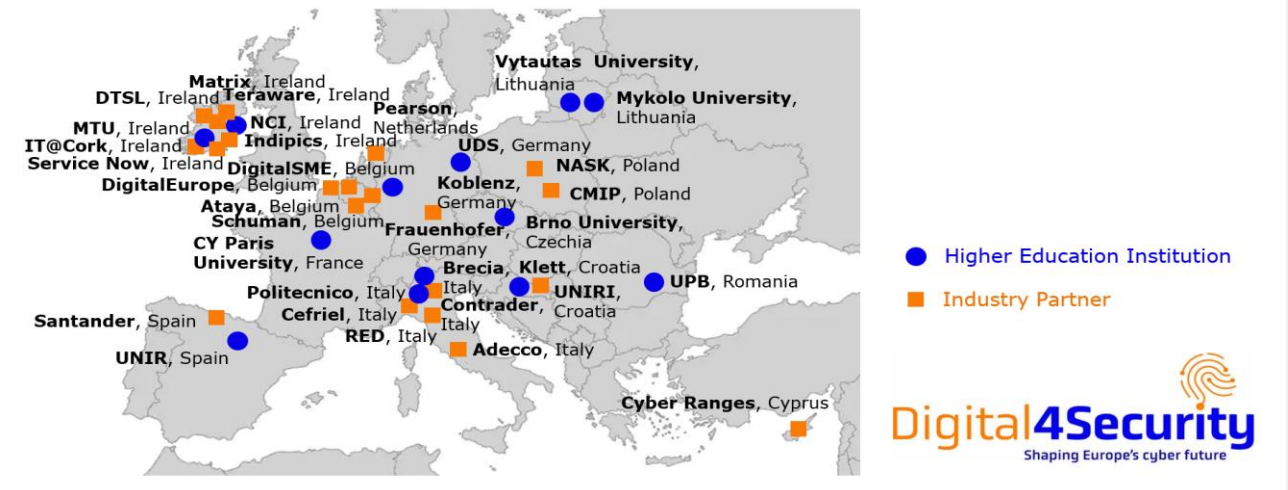
The Joint Master's Programme in **Cybersecurity Management and Data Sovereignty** is a 60 ECTS, fully online degree jointly awarded by the German University of Digital Science (UDS, Germany), Munster Technological University (MTU, Ireland), and Universidad Internacional de La Rioja (UNIR, Spain).

The programme has been created within the framework of the **Digital4Security** project (Grant Agreement No. 101123430), co-funded by the European Union under the *DIGITAL Europe Programme* (DIGITAL-2022-SKILLS-03 – Advanced Digital Skills).

Designed to meet Europe's growing demand for strategic cybersecurity expertise, the programme combines academic excellence with strong industry relevance. It supports professionals in developing the advanced competencies required to lead cybersecurity efforts across public and private sectors, particularly in Small and Medium-Sized Enterprises (SMEs) and critical infrastructure domains.

Figure 1 illustrates the partners involved in the Digital4Security project. Students gain access to this network of cybersecurity excellence upon enrolling in the Master's programme.

Figure 1: Digital4Security Partner Network.



A systematic overview of the Digital4Security partners is provided in Table 1.

Table 1: The Digital4Security Network – Higher Education Institutions (HEIs) and Associate Partners (Listed Alphabetically)

No.	Partner	Abbreviation	Country	Role
1	Adecco Formazione SRL	ADECCO TRAINING	Italy	Associate partner
2	Adecco Italia Holding di Partecipazione e Servizi SPA	ADECCO GROUP	Italy	Associate partner
3	Adecco Italia	ADECCO ITALIA	Italy	Associate partner
4	Ataya & Partners	ATAYA	Belgium	Associate partner
5	Banco Santander SA	BANCO SANTANDER	Spain	Associate partner
6	Brno University of Technology	BRNO	Czech Republic	HEI partner
7	Cefriel Società Consortile a Responsabilità Limitata Società Benefit	CEFRIEL	Italy	Associate partner
8	CMIP (Polski Klaster Cyberbezpieczenstwa CyberMadeInPoland Sp. z o. o.)	CMIP	Poland	Associate partner
9	Contrader SRL	CONTRADER	Italy	Associate partner
10	CY Cergy Paris Université	CY	France	HEI partner
11	Cyber Ranges Ltd	CYBER RANGES	Cyprus	Associate partner
12	DigitalEurope AISBL	DIGITALEUROPE	Belgium	Associate partner
13	Digital Technology Skills Limited	DTSL	Ireland	Associate partner
14	European Digital SME Alliance	DIGITAL SME	Belgium	Associate partner
15	Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung EV	FHG	Germany	Associate partner
16	German University of Digital Science	UDS	Germany	HEI partner
17	Independent Pictures Limited	INDIEPICS	Ireland	Associate partner
18	IT@Cork Association Limited LBG	IT@CORK	Ireland	Associate partner

No.	Partner	Abbreviation	Country	Role
19	Matrix Internet Applications Limited	MATRIX	Ireland	Associate partner
20	Munster Technological University	MTU	Ireland	HEI partner
21	Mykolo Romerio Universitetas	MRU	Lithuania	HEI partner
22	National College of Ireland	NCI	Ireland	HEI partner
23	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	NASK	Poland	Associate partner
24	Pearson Benelux	PEARSON B.	Netherlands	Associate partner
25	Politecnico di Milano	POLIMI	Italy	HEI partner
26	Profil Klett d.o.o.	PROFIL KLETT	Croatia	Associate partner
27	Red Open S.R.L.	RED OPEN S.R.L.	Italy	Associate partner
28	Schuman Associates SCRL	SA	Belgium	Associate partner
29	ServiceNow Ireland Limited	ServiceNow	Ireland	Associate partner
30	Skillnet Ireland Company Limited By Guarantee	SKILLNET	Ireland	Associate partner
31	Terawe Technologies Limited	TERAWE	Ireland	Associate partner
32	Universidad Internacional de La Rioja	UNIR	Spain	HEI partner
33	Università degli Studi di Brescia	UNIBS	Italy	HEI partner
34	Universitatea Națională de Știință și Tehnologie Politehnica București	UPB	Romania	HEI partner
35	Universität Koblenz	UNI KO	Germany	HEI partner
36	University of Rijeka	UNIRI	Croatia	HEI partner
37	Vytautas Magnus University	VMU	Lithuania	HEI partner

1. How to Use this Guide on Pathway and Module Selection

At the very beginning of your studies, upon admission to the programme, you will be invited to select a **professional profile** and to **choose modules** for your first term.

This guide is designed to support you in making these decisions. It provides **Profile Roadmaps** that explain the focus of each professional profile, outline recommended module sequences, and illustrate how your prior academic and professional background may influence which options may be most suitable for you, and when particular modules might best be taken.

The guidance offered here is **advisory**. Its purpose is to help you plan a coherent, realistic, and rewarding study pathway that fully aligns with your experience, interests, and professional goals. This Guide does not make decisions on your behalf. Rather, it aims to **empower you to make well-informed decisions** for yourself, in line with your personal priorities and circumstances.

2. Recognising the Value of Different Professional Backgrounds

The Master's programme in Cybersecurity Management and Data Sovereignty is explicitly designed for a **diverse cohort of learners**. Admission is open to graduates from all disciplines, while the curriculum deliberately integrates **managerial, technical, organisational, legal, and societal perspectives**.

Different academic and professional backgrounds are therefore **not a limitation to be overcome**, but a resource to be actively leveraged. Examples include:

- **Technically oriented participants** (e.g. engineers, analysts, developers), who bring depth in systems, tools, and technical architectures;
- **Managerial professionals**, contributing experience in governance, strategic decision-making, and organisational change;
- **Legal, policy, or compliance specialists**, offering expertise in regulation, accountability, risk, and institutional frameworks;
- **Educators**, contributing strengths in pedagogy, training, communication, awareness-building, and knowledge transfer;
- **Hybrid profiles**, combining several of the above through interdisciplinary study or professional practice.

Throughout the programme, you are encouraged to reflect on how your background shapes:

- The topics, questions, and goals you find most relevant;
- The problems you are particularly well placed to analyse;
- The perspectives you bring to discussions and assessments.

This reflective awareness is not only personally beneficial; it is a **core academic competence at Master's level**, closely aligned with the programme's learning outcomes related to critical thinking, leadership, and self-directed learning.

Beyond academic work, you are strongly encouraged to make use of the opportunities offered during your studies – and later through the alumni network – to build **collegial relationships**. Engaging with peers from different backgrounds reflects real-world professional practice, particularly in industry contexts, where complex challenges require multiple forms of expertise.

Especially valuable skills to develop include:

- Learning to communicate across the "languages" of different disciplines;
- Recognising and leveraging complementary strengths within a team;
- Actively seeking diverse expert perspectives within a project to identify risks and opportunities more comprehensively;
- Collaborating – recognising that complex problems are often best addressed not through individual work alone (typically within one area of expertise, or with a limited set of specialities), but by working together with others to broaden and deepen the team's collective expertise.

Many students find that such diverse professional connections lead to **unexpected and lasting professional opportunities**.

3. Common Foundation for All Profiles: Mandatory Taught Modules (15 ECTS)

All students need to complete **three mandatory taught modules**. It is recommended to complete these modules early during your studies, as they establish a shared conceptual and methodological foundation across the cohort. Particulalry full-time students should **take them in the first and second term**.

Students with a strong technical background may choose to take the technically oriented mandatory module **Ethical Hacking & Penetration Testing** at any point. Students from non-technical backgrounds may find it beneficial to begin with the less technically intensive mandatory modules, namely **Communication Design for Cybersecurity** and **Business Resilience, Threat Response & Incident Management**. This approach allows students with limited prior technical training to use their first term to engage with the self-study materials provided in the **Welcome Module**, supporting a gradual and well-prepared introduction to technical concepts before progressing to more technically demanding coursework.

Please note that, in order to start the **Master's Thesis**, students must have completed **at least two mandatory taught modules** and a **minimum of 30 ECTS in total** (see *Study and Examination Regulations*, Annex 2, and the *Module Handbook*, Annex 7).

For full-time students aiming to complete the programme within one year, this means that at least two mandatory modules need to be completed within the first two terms in order to be on track.

4. Choice of Elective Modules

When deciding which elective modules to take, and at what stage of the programme, the following guiding principles may be helpful:

- **Align module choices with your professional goals.** Select modules that support your intended career direction, professional profile, or anticipated role development.
- **Prioritise passion.** Courses that genuinely spark your enthusiasm are often those in which sustained effort and high-quality outcomes build most naturally.
- **Adopt a study strategy that suits your learning style.** Students differ in how they prefer to structure their workload. Common approaches include:
    - Some students prefer to **build confidence in the first term**, becoming familiar with academic procedures and expectations by selecting modules they anticipate to be introductory or of moderate difficulty.
    - Others prefer to **address the most demanding modules early**, allowing subsequent terms to feel more manageable once the most challenging elements are completed.
- **If neither approach strongly appeals to you, aim for balance.** The academic calendar is published at least one year in advance, allowing you to plan your studies beyond a single term. A balanced approach may involve combining:
    - one module anticipated to be less demanding with
    - one module expected to require greater effort in each teaching term, thereby avoiding large fluctuations in workload intensity.
- **Plan ahead with your Master's thesis in mind.** If you already have an emerging thesis topic or area of interest, consider which module can provide essential theoretical foundations, methodological skills, or domain knowledge, and ensure to complete it before the thesis phase.
- **Be realistic about cumulative workload.** While ambition is encouraged, over-concentration of demanding modules in a single term may negatively affect your learning experience. Realistic sequencing supports both academic performance and well-being.

5. What if I Want to Revise My Choices?

Learning may be accompanied by a more refined understanding of which topics suit you best and how you learn most effectively. The programme therefore allows some flexibility to adjust your choices.

5.1 Changing Module Registrations

Changes to module enrolment are possible provided that you have not yet attempted, or missed, any assessment that contributes to grading. In practice, this means that you can usually change your module selection up to **Day 4 of the teaching term**, as lecturers are instructed not to require any grading-relevant submissions before **Day 5**.

The first week of each module is designed to give you an initial impression of the course and to provide a detailed overview of what lies ahead. You are encouraged to use this period actively and to make corrective decisions early if a module does not align with your expectations or learning goals.

Across the entire programme, students are granted **up to ten module re-registrations**. This means that while it is not possible to sample a large number of modules casually and change enrolments frequently, you do retain the ability to make adjustments in cases where this is genuinely important. This balance ensures both individual flexibility and stable learning environments that support effective coursework from the first teaching week.

Unenrolment from a module counts as **one re-registration**, and enrolling in a different module counts as **a second re-registration**. For example, if you enrol in Module A and decide by Day 2 that it is not suitable, withdrawing from the module uses one of your ten permitted re-registrations, leaving you with nine remaining. If you then enrol in Module B on Day 3, this constitutes a second change to your

original registrations for the teaching term, leaving you with eight re-registrations available.

5.2 Changing Professional Profiles

It is also possible to change your selected **Professional Profile** during your studies.

As outlined in the *Student Handbook* (Annex 7), you may choose a Professional Pathway during the admission process by selecting the profile that best aligns with your career goals. If you did not select a pathway at admission, you may do so at a later stage by contacting the **Programme Coordinator of the university curating your preferred profile (cf. Sect 12)**.

If your professional objectives evolve over time, you are welcome to change your selected profile. To do so, please contact **both Programme Coordinators** – the coordinator of the profile you wish to leave and the coordinator of the profile you wish to join – by sending a **single email addressed to both**. This ensures a smooth transition and appropriate documentation of your updated study focus.

Choosing a professional profile is optional. If you prefer, you may freely select all 30 ECTS of elective modules without committing to a specific pathway. However, students are strongly encouraged to align their module choices with an intended career direction by selecting a profile, ideally already at the point of admission. Doing so provides access to more targeted preparation, academic guidance, and career-oriented support throughout the programme. It also enables clearer documentation of your area of specialisation in the Diploma Supplement, which may be of value to future employers or for further academic progression.

Professional profile registrations may be changed **up to three times** over the course of the programme. A change from Profile A to Profile B, from no profile selection to Profile A, or from Profile A to no profile selection each counts as **one profile change** against the three available.

6. Characterization of Professional Profiles

The Digital4Security Master's Programme is designed to support students with diverse professional backgrounds, while remaining closely aligned with the evolving demands of the European cybersecurity landscape. You are encouraged to enroll in **one professional profile** to guide your learning, selected from **six profiles supported by the programme**. Enrolling in more than one profile is not possible.

Further guidance on professional profiles within the programme is provided in the *Module Handbook* (Annex 7) and the *Student Handbook* (Annex 8).

Below, you will find the **official ENISA characterisations** of the six roles supported by the Master's programme.

CHIEF INFORMATION SECURITY OFFICER (CISO)

Alternative Title(s)

Cybersecurity Programme Director
Information Security Officer (ISO)
Information Security Manager
Head of Information Security
IT/ICT Security Officer

Summary statement

Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.

Mission

Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.

Deliverable(s)

- Cybersecurity Strategy
- Cybersecurity Policy

Main task(s)

- Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives
- Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution
- Supervise the application and improvement of the Information Security Management System (ISMS)
- Educate senior management about cybersecurity risks, threats and their impact to the organization
- Ensure the senior management approves the cybersecurity risks of the organisation
- Develop cybersecurity plans
- Develop relationships with cybersecurity-related authorities and communities
- Report cybersecurity incidents, risks, findings to the senior management
- Monitor advancement in cybersecurity
- Secure resources to implement the cybersecurity strategy
- Negotiate the cybersecurity budget with the senior management

Key skill(s)	• Ensure the organisation's resiliency to cyber incidents • Manage continuous capacity building within the organisation • Review, plan and allocate appropriate cybersecurity resources • Assess and enhance an organisation's cybersecurity posture • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Analyse and comply with cybersecurity-related laws, regulations and legislations • Implement cybersecurity recommendations and best practices • Manage cybersecurity resources • Develop, champion and lead the execution of a cybersecurity strategy • Influence an organisation's cybersecurity culture • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Review and enhance security documents, reports, SLAs and ensure the security objectives • Identify and solve cybersecurity-related issues • Establish a cybersecurity plan • Communicate, coordinate and cooperate with internal and external stakeholders • Anticipate required changes to the organisation's information security strategy and formulate new plans

e-Competences (from e-CF)		
	A.7. Technology Trend Monitoring	Level 4
	D.1. Information Security Strategy Development	Level 5
	E.3. Risk Management	Level 4
	E.8. Information Security Management	Level 4
	E.9. IS-Governance	Level 5

CYBERSECURITY EDUCATOR

Alternative Title(s)	Cybersecurity Awareness Specialist Cybersecurity Trainer Faculty in Cybersecurity (Professor, Lecturer)
Summary statement	Improves cybersecurity knowledge, skills and competencies of humans.
Mission	Designs, develops and conducts awareness, training and educational programmes in cybersecurity and data protection-related topics. Uses appropriate teaching and training methods, techniques and instruments to communicate and enhance the cybersecurity culture, capabilities, knowledge and skills of human resources. Promotes the importance of cybersecurity and consolidates it into the organisation.
Deliverable(s)	• Cybersecurity Awareness Program • Cybersecurity Training Material
Main task(s)	• Develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need • Organise, design and deliver cybersecurity and data protection awareness-raising activities, seminars, courses, practical training • Monitor, evaluate and report training effectiveness • Evaluate and report trainee's performance • Finding new approaches for education, training and awareness-raising • Design, develop and deliver cybersecurity simulations, virtual labs or cyber range environments • Provide guidance on cybersecurity certification programs for individuals • Continuously maintain and enhance expertise; encourage and empower continuous enhancement of cybersecurity capacities and capabilities building
Key skill(s)	• Identify needs in cybersecurity awareness, training and education • Design, develop and deliver learning programmes to cover cybersecurity needs • Develop cybersecurity exercises including simulations using cyber range environments

Key knowledge	• Provide training towards cybersecurity and data protection professional certifications • Utilise existing cybersecurity-related training resources • Develop evaluation programs for the awareness, training and education activities • Communicate, present and report to relevant stakeholders • Identify and select appropriate pedagogical approaches for the intended audience • Motivate and encourage people • Pedagogical standards, methodologies and frameworks • Cybersecurity awareness, education and training programme development • Cybersecurity-related certifications • Cybersecurity education and training standards, methodologies and frameworks • Cybersecurity related laws, regulations and legislations • Cybersecurity recommendations and best practices • Cybersecurity standards, methodologies and frameworks • Cybersecurity controls and solutions	
e-Competences (from e-CF)	D.3. Education and Training Provision	Level 3
	D.9. Personnel Development	Level 3
	E.8. Information Security Management	Level 3

CYBER LEGAL, POLICY & COMPLIANCE OFFICER

Alternative Title(s)

Data Protection Officer (DPO)
Privacy Protection Officer
Cyber Law Consultant
Cyber Legal Advisor
Information Governance Officer
Data Compliance Officer
Cybersecurity Legal Officer
IT/ICT Compliance Manager
Governance Risk Compliance (GRC) Consultant

Summary statement

Manages compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organisation's strategy and legal requirements.

Mission

Oversees and assures compliance with cybersecurity- and data-related legal, regulatory frameworks and policies in line with the organisation's strategy and legal requirements. Contributes to the organisation's data protection related actions. Provides legal advice in the development of the organisation's cybersecurity governance processes and recommended remediation strategies/solutions to ensure compliance.

Deliverable(s)

- Compliance Manual
- Compliance Report

Main task(s)

- Ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations
- Identify and document compliance gaps
- Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures
- Enforce and advocate organisation's data privacy and protection program
- Ensure that data owners, holders, controllers, processors, subjects, internal or external partners and entities are informed about their data protection rights, obligations and responsibilities
- Act as a key contact point to handle queries and complaints regarding data processing

	• Assist in designing, implementing, auditing and compliance testing activities in order to ensure cybersecurity and privacy compliance • Monitor audits and data protection related training activities • Cooperate and share information with authorities and professional groups • Contribute to the development of the organisation's cybersecurity strategy, policy and procedures • Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization • Manage legal aspects of information security responsibilities and third-party relations
Key skill(s)	• Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements • Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy • Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties • Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools • Explain and communicate data protection and privacy topics to stakeholders and users • Understand, practice and adhere to ethical requirements and standards • Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies • Collaborate with other team members and colleagues
Key knowledge	• Cybersecurity related laws, regulations and legislations • Cybersecurity standards, methodologies and frameworks

	• Cybersecurity policies • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Privacy impact assessment standards, methodologies and frameworks	
e-Competences (from e-CF)	A.1. Information Systems and Business Strategy Alignment	Level 4
	D.1. Information Security Strategy Development	Level 4
	E.8. Information Security Management	Level 3
	E.9. IS-Governance	Level 4

CYBERSECURITY RISK MANAGER

Alternative Title(s)	Information Security Risk Analyst Cybersecurity Risk Assurance Consultant Cybersecurity Risk Assessor Cybersecurity Impact Analyst Cyber Risk Manager
Summary statement	Manage the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop, maintain and communicate the risk management processes and reports.
Mission	Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organisation and ensures that risks remain at an acceptable level for the organisation by selecting mitigation actions and controls.
Deliverable(s)	• Cybersecurity Risk Assessment Report • Cybersecurity Risk Remediation Action Plan
Main task(s)	• Develop an organisation's cybersecurity risk management strategy • Manage an inventory of organisation's assets • Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems • Identification of threat landscape including attackers' profiles and estimation of attacks' potential • Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy • Monitor effectiveness of cybersecurity controls and risk levels • Ensure that all cybersecurity risks remain at an acceptable level for the organisation's assets • Develop, maintain, report and communicate complete risk management cycle

Key skill(s)	• Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards • Analyse and consolidate organisation's quality and risk management practices • Enable business assets owners, executives and other stake-holders to make risk-informed decisions to manage and mitigate risks • Build a cybersecurity risk-aware environment • Communicate, present and report to relevant stakeholders • Propose and manage risk-sharing options	
Key knowledge	• Risk management standards, methodologies and frame-works • Risk management tools • Risk management recommendations and best practices • Cyber threats • Computer systems vulnerabilities • Cybersecurity controls and solutions • Cybersecurity risks • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Cybersecurity-related certifications • Cybersecurity-related technologies	
e-Competences (from e-CF)	E.3. Risk Management	Level 4
	E.5. Process Improvement	Level 3
	E.7. Business Change Management	Level 4
	E.9. IS-Governance	Level 4

CYBER THREAT INTELLIGENCE SPECIALIST

Alternative Title(s)	Cyber Intelligence Analyst Cyber Threat Modeller
Summary statement	Collect, process, analyse data and information to produce actionable intelligence reports and disseminate them to target stakeholders.
Mission	Manages cyber threat intelligence life cycle including cyber threat information collection, analysis and production of actionable intelligence and dissemination to security stakeholders and the CTI community, at a tactical, operational and strategic level. Identifies and monitors the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors and their trends, track threat actors' activities and observe how non-cyber events can influence cyber-related actions.
Deliverable(s)	• Cyber Threat Intelligence Manual • Cyber Threat Report
Main task(s)	• Develop, implement and manage the organisation's cyber threat intelligence strategy • Develop plans and procedures to manage threat intelligence • Translate business requirements into Intelligence Requirements • Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders • Identify and assess cyber threat actors targeting the organisation • Identify, monitor and assess the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors by analysing open-source and proprietary data, information and intelligence • Produce actionable reports based on threat intelligence data • Elaborate and advise on mitigation plans at the tactical, operational and strategic level • Coordinate with stakeholders to share and consume intelligence on relevant cyber threats

	• Leverage intelligence data to support and assist with threat modelling, recommendations for Risk Mitigation and cyber threat hunting • Articulate and communicate intelligence openly and publicly at all levels • Convey the proper security severity by explaining the risk exposure and its consequences to non-technical stakeholders	
Key skill(s)	• Collaborate with other team members and colleagues • Collect, analyse and correlate cyber threat information originating from multiple sources • Identify threat actors TTPs and campaigns • Automate threat intelligence management procedures • Conduct technical analysis and reporting • Identify non-cyber events with implications on cyber-related activities • Model threats, actors and TTPs • Communicate, coordinate and cooperate with internal and external stakeholders • Communicate, present and report to relevant stakeholders • Use and apply CTI platforms and tools	
Key knowledge	• Operating systems security • Computer networks security • Cybersecurity controls and solutions • Computer programming • Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks • Responsible information disclosure procedures • Cross-domain and border-domain knowledge related to cybersecurity • Cyber threats • Cyber threat actors • Cybersecurity attack procedures • Advanced and persistent cyber threats (APT) • Threat actors Tactics, Techniques and Procedures (TTPs) • Cybersecurity-related certifications	
e-Competences (from e-CF)	B.5. Documentation Production	Level 3
	D.7. Data Science and Analytics	Level 4

D.10. Information and Knowledge Management	Level 4
E.4. Relationship Management	Level 3
E.8. Information Security Management	Level 4

CYBERSECURITY AUDITOR

Alternative Title(s)	Information Security Auditor (IT or Legal Auditor) Governance Risk Compliance (GRC) Auditor Cybersecurity Audit Manager Cybersecurity Procedures and Processes Auditor Information Security Risk and Compliance Auditor Data Protection Assessment Analyst
Summary statement	Perform cybersecurity audits on the organisation's ecosystem. Ensuring compliance with statutory, regulatory, policy information, security requirements, industry standards and best practices.
Mission	Conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organisation's legal and regulatory frameworks policies. Evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations.
Deliverable(s)	• Cybersecurity Audit Plan • Cybersecurity Audit Report
Main task(s)	• Develop the organisation's auditing policy, procedures, standards and guidelines • Establish the methodologies and practices used for systems auditing • Establish the target environment and manage auditing activities • Define audit scope, objectives and criteria to audit against • Develop an audit plan describing the frameworks, standards, methodology, procedures and auditing tests • Review target of evaluation, security objectives and requirements based on the risk profile • Audit compliance with cybersecurity-related applicable laws and regulations • Audit conformity with cybersecurity-related applicable standards • Execute the audit plan and collect evidence and measurements • Maintain and protect the integrity of audit records

	• Develop and communicate conformity assessment, assurance, audit, certification and maintenance reports • Monitor risk remediation activities	
Key skill(s)	• Organise and work in a systematic and deterministic way based on evidence • Follow and practice auditing frameworks, standards and methodologies • Apply auditing tools and techniques • Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls • Decompose and analyse systems to identify weaknesses and ineffective controls • Communicate, explain and adapt legal and regulatory requirements and business needs • Collect, evaluate, maintain and protect auditing information • Audit with integrity, being impartial and independent	
Key knowledge	• Cybersecurity controls and solutions • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Conformity assessment standards, methodologies and frameworks • Auditing standards, methodologies and frameworks • Cybersecurity standards, methodologies and frameworks • Auditing-related certification • Cybersecurity-related certifications	
e-Competences (from e-CF)	B.3. Testing	Level 4
	B.5. Documentation Production	Level 3
	E.3. Risk Management	Level 4
	E.6 ICT Quality Management	Level 4

7. Selecting Modules and Pathways to Build Your Portfolio

You are encouraged to view the programme as both:

- a space to build on and deepen your existing knowledge and expertise; as well as
- an opportunity to extend and challenge that expertise by engaging with new perspectives and domains.

As you plan your studies, it can be helpful to strike a balance between demonstrating confidence in your established professional identity and providing evidence of growth, integration, and interdisciplinary learning.

When making choices about modules and pathways, it may be useful to think in terms of two broad poles of possibility, between which you can intentionally position yourself:

- **Lower effort, moderate development**: deepening your existing professional trajectory while cautiously extending into new areas; or
- **Higher effort, extensive development**: deliberately investing time in building a new, complementary area of in-depth expertise alongside your original background.

There is no "right" or "wrong" choice. What matters is that your decision is intentional and well informed, with a clear understanding of the implications for workload, learning strategy, and outcomes.

To support this process, the professional profiles are accompanied by a colour-coded orientation system:

- **Green** indicates that a profile is typically more accessible for students with a particular background;

- **Yellow** indicates that moderate additional effort may be required;
- **Purple** indicates that the profile may be more demanding and may require additional preparation time for students without prior exposure to the relevant domain.

Please note that the **colour coding of effort and difficulty** reflects indicative estimations within the programme. Individual perceptions and learning experiences may vary. The colours should therefore be understood as **general guidance rather than definitive classifications**. As the programme is delivered and evaluated, aggregated student feedback on workload and perceived difficulty is used to refine these colour-coded recommendations.

For example, if your previous education and professional experience are non-technical and you select a technically intensive profile such as *Cyber Threat Intelligence Specialist*, you should typically expect to invest additional time in preparatory reading, familiarisation with technical concepts, and the completion of coursework.

As explained in Section 11, upon admission you gain access to the **Welcome Module**, which includes short self-assessment tests for modules with specified prerequisites. These self-tests are designed to help you assess whether you meet the expected entry level. Where gaps are identified, the module provides curated self-study materials to support effective preparation before enrolling in the relevant module.

If several gaps are identified, working through the preparation materials may itself require significant time. You are therefore encouraged to take this into account when planning your study pathway and overall workload.

8. Effort Estimates for Professional Profiles Based on Student Backgrounds

Below you find indicators as to how much effort the professional profiles may typically involve for students of different backgrounds. They are intended as **orientation tools**, and should not be perceived as barriers.

Furthermore, it is recommended to read the tables below alongside the full module information included in the *Module Handbook* (Annex 7), to use the self-assessment tools in the Welcome Module, and to discuss options with the study-affairs team, or profile coordinator as appropriate, in order to plan an effective, sustainable and enjoyable learning pathway.

Chief Information Security Officer (CISO) – Estimated Difficulty by Student Background

Student Background	Expected Difficulty
IT professionals	Green
Managerial professionals	Green
Legal, policy, or compliance specialists	Yellow
Educators	Yellow

Explanation:

The CISO profile is inherently interdisciplinary, combining strategic leadership, governance, risk management, and technical literacy.

IT professionals and managers typically find this profile accessible, as it builds either on technical depth expanded towards strategy, or on leadership experience enriched with cybersecurity governance.

Legal and compliance specialists may require additional effort to strengthen their understanding of technical and managerial concepts.

Educators may need to deepen both organisational governance and applied security management aspects.

Cybersecurity Educator
– Estimated Difficulty by Student Background

Student Background	Expected Difficulty
IT professionals	Yellow
Managerial professionals	Yellow
Legal, policy, or compliance specialists	Yellow
Educators	Green

Explanation:

This profile is highly accessible to students with prior teaching, training, or instructional design experience. Educators benefit from strong alignment with pedagogical standards and learning design.

IT professionals, managers, and legal specialists may need to invest additional effort in didactics, assessment design, and educational methodologies, even though their domain knowledge is typically strong and useful.

Conversely, non-technical educators may need to deepen their cybersecurity content knowledge to reach the expected professional standard.

Cyber Legal, Policy & Compliance Officer – Estimated Difficulty by Student Background

Student Background	Expected Difficulty
IT professionals	Yellow
Managerial professionals	Yellow
Legal, policy, or compliance specialists	Green
Educators	Purple

Explanation:

This profile is most naturally aligned with students from legal, policy, regulatory, or compliance backgrounds, who already possess familiarity with statutory interpretation, governance structures, and regulatory reasoning.

IT professionals and managers typically need to invest effort in understanding legal frameworks, compliance logic, and formal documentation practices.

Educators may need to strengthen both legal reasoning and applied organisational perspectives.

Cybersecurity Risk Manager – Estimated Difficulty by Student Background

Student Background	Expected Difficulty
IT professionals	Green
Managerial professionals	Yellow
Legal, policy, or compliance specialists	Yellow
Educators	Purple

Explanation:

The Cybersecurity Risk Manager profile strongly integrates technical system understanding with structured risk frameworks and business decision-making.

IT professionals usually find this profile accessible, as they can extend existing system knowledge into formal risk analysis and control evaluation.

Managers and legal/compliance specialists often need to strengthen their understanding of technical vulnerabilities and threat landscapes.

Educators may face the highest entry effort, as the role requires the integration of technical risk expertise with organisational processes.

Cyber Threat Intelligence Specialist – Estimated Difficulty by Student Background

Student Background	Expected Difficulty
IT professionals	Green
Managerial professionals	Purple
Legal, policy, or compliance specialists	Purple
Educators	Purple

Explanation:

This is the most technically intensive profile in the Master's programme.

IT professionals with backgrounds in networks, systems, security operations, or data analysis are best positioned to engage with core concepts, tooling, and analytical workflows.

For managers, legal specialists, and educators, the profile typically requires substantial additional effort, including developing technical literacy, understanding threat actor behaviour, and working with specialised intelligence platforms and data sources.

Cybersecurity Auditor
– Estimated Difficulty by Student Background

Student Background	Expected Difficulty
IT professionals	Yellow
Managerial professionals	Yellow
Legal, policy, or compliance specialists	Green
Educators	Purple

Explanation:

The Cybersecurity Auditor profile sits at the intersection of technical controls, regulatory requirements, and formal assurance methodologies.

Legal and compliance specialists typically find this profile accessible due to their familiarity with standards, evidence-based reasoning, and regulatory frameworks.

IT professionals and managers usually need to adapt from implementation or leadership roles to an independent, evidence-driven audit mindset.

Educators may face higher effort due to the need to master both technical control evaluation and formal auditing standards.

9. Choosing Modules within a Professional Profile

For each professional profile, a set of recommended modules is provided. Completing **at least 20 ECTS (four modules of 5 ECTS each)** from the recommended modules of your chosen pathway, together with completion of the **Master's thesis (15 ECTS)** on a profile-aligned topic, qualifies you for formal recognition of that professional profile in your **Diploma Supplement**.

The tables below list the recommended modules for each profile together with **indicative effort estimates**, using the same colour-coding system introduced earlier (Sect. 7). These estimates reflect typical starting points for different student backgrounds and are intended to support **study planning, workload management, and expectation setting**.

They also allow you to fine-tune the level of challenge and professional development you wish to pursue relative to your original entry profile.

For example, if you have a non-technical professional background (such as *Business Management*) and choose a technically demanding profile (such as *Cyber Threat Intelligence Specialist*), this would overall constitute a **"purple" choice**, reflecting an expectation of substantial effort, accompanied by significant personal and professional development into largely new areas of knowledge. Within that profile, however, you still retain flexibility: Some recommended modules are marked as **yellow**, allowing you to prioritise options that are comparatively less demanding while still contributing towards profile recognition.

Conversely, you may also choose to **increase the level of challenge within an otherwise accessible profile**. For instance, if your professional background is in *Education* and you select the *Cybersecurity Educator* profile, this represents a **"green" choice**, as the pathway builds directly on existing pedagogical strengths without requiring in-depth mastery of an entirely new domain. Nevertheless, several recommended modules within this profile are also marked **yellow** for educators. By

prioritising these modules, you can deliberately extend your expertise into new thematic or methodological areas, should you wish to do so.

As noted previously, these colour codings are **internal orientation estimates** and may not apply uniformly to every individual learner. They will be further refined over time based on aggregated student feedback collected through post-course surveys, as well as course progression data. In all cases, students are strongly encouraged to consult the *Module Handbook* (Annex 7) for detailed information on module content, learning outcomes, assessment formats, and prerequisites, in order to assess the relevance and anticipated effort of each module in light of their own background and learning objectives.

Chief Information Security Officer (CISO) – Estimated Module Effort

Focus: leadership, governance, resilience, communication, strategic decision-making

	Student Background			
Recommended Module	**Computer Science**	**Manage-ment**	**Legal / Compliance**	**Educators**
Cybersecurity Culture, Strategy & Leadership	Green	Green	Yellow	Yellow
Law, Compliance, Governance, Policy, and Ethics	Yellow	Green	Green	Yellow
Cybersecurity Economics & Supply Chain	Yellow	Green	Yellow	Yellow
Risk Management of Cyber-Physi-cal Systems	Green	Yellow	Yellow	Purple
CISO and Crisis Communication	Green	Green	Yellow	Yellow
AI & Emerging Topics in Cyberse-curity	Green	Purple	Purple	Purple

Cybersecurity Educator – Estimated Module Effort

Focus: pedagogy, training delivery, research methods, interdisciplinary understanding

	Student Background			
Recommended Module	**Computer Science**	**Management**	**Legal / Compliance**	**Educators**
Cybersecurity Education & Training Delivery I	Yellow	Yellow	Yellow	Green
Cybersecurity Education & Training Delivery II	Yellow	Yellow	Yellow	Green
Cybersecurity Culture, Strategy & Leadership	Green	Green	Yellow	Yellow
Research Methods	Yellow	Yellow	Yellow	Green
Law, Compliance, Governance, Policy, and Ethics	Yellow	Green	Green	Yellow
AI & Emerging Topics in Cybersecurity	Green	Purple	Purple	Purple

Cyber Legal, Policy & Compliance Officer – Estimated Module Effort

Focus: legal frameworks, data sovereignty, ethics, governance, compliance operations

	Student Background			
Recommended Module	**Computer Science**	**Management**	**Legal / Compliance**	**Educators**
Law, Compliance, Governance, Policy, and Ethics	Yellow	Green	Green	Yellow
Cybersecurity Auditing	Yellow	Yellow	Green	Purple
Cybersecurity Law and Data Sovereignty	Yellow	Yellow	Green	Yellow
AI & Emerging Topics in Cybersecurity	Green	Purple	Purple	Purple
Digital Forensics, Chain of Custody and eDiscovery	Green	Purple	Yellow	Purple

Cybersecurity Risk Manager – Estimated Module Effort

Focus: risk assessment, systems-level thinking, compliance, crisis response

	Student Background			
Recommended Module	**Computer Science**	**Manage-ment**	**Legal / Compliance**	**Educators**
Risk Management of Cyber-Physi-cal Systems	Green	Yellow	Yellow	Purple
Cybersecurity Economics & Supply Chain	Yellow	Green	Yellow	Yellow
Security Operations	Green	Yellow	Purple	Purple
Technological Foundations in CS & Security Controls	Green	Yellow	Yellow	Yellow
Law, Compliance, Governance, Policy, and Ethics	Yellow	Green	Green	Yellow
AI & Emerging Topics in Cyberse-curity	Green	Purple	Purple	Purple

Cyber Threat Intelligence Specialist – Estimated Module Effort

Focus: offensive/defensive tactics, malware, threat detection, data-driven analysis

	Student Background			
Recommended Module	**Computer Science**	**Management**	**Legal / Compliance**	**Educators**
Threat Intelligence	Yellow	Purple	Purple	Purple
Technological Foundations in CS & Security Controls	Green	Yellow	Yellow	Yellow
Security Operations	Green	Yellow	Purple	Purple
Automation of Security Tasks and Data Analytics	Green	Purple	Purple	Purple
Malware Analysis	Yellow	Purple	Purple	Purple
Enterprise Architecture, Infrastructure Design and Cloud Computing	Green	Yellow	Purple	Purple

Cybersecurity Auditor – Estimated Module Effort

Focus: auditing practices, compliance, forensic readiness, technical documentation

	Student Background			
Recommended Module	**Computer Science**	**Management**	**Legal / Compliance**	**Educators**
Cybersecurity Auditing	Yellow	Yellow	Green	Purple
Law, Compliance, Governance, Policy, and Ethics	Yellow	Green	Green	Yellow
Cybersecurity Law and Data Sovereignty	Yellow	Yellow	Green	Yellow
Risk Management of Cyber-Physical Systems	Green	Yellow	Yellow	Purple
Security Operations	Green	Yellow	Purple	Purple
Digital Forensics, Chain of Custody and eDiscovery	Green	Purple	Yellow	Purple

10. Pathways for Meeting Course Prerequisites

Another important aspect of course sequencing is the consideration of **prerequisite knowledge**, which may influence when certain modules are most appropriately taken. A related consideration is how you prefer to prepare for more demanding modules, particularly those that specify entry expectations.

Educational offerings within the 60-ECTS Online Master's Programme are open both to Master's students and to Microcredential learners. As Microcredential learners enrol in individual modules without pursuing the full Master's degree, prior completion of other Master's modules is **never a mandatory entry requirement** for any course.

Accordingly, the *Module Handbook* (Annex 7) consistently clarifies that students may meet the expected entry knowledge for a module in different ways. This may be achieved either by completing the recommended prerequisite module within the Master's programme or through alternative routes, such as already possessing the relevant knowledge, or developing it independently through self-directed study.

An overview of the **specific prerequisites** listed in the *Module Handbook* is provided in Table 1. Modules that do not specify prerequisites are omitted in this list.

Table 1. Overview of Prerequisites listed in the Module Handbook

Module	Prerequisites specified in the Module Handbook
Ethical Hacking & Penetration Testing	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.
AI & Emerging Topics in Cybersecurity	Recommended, not required: • Security Operations • Machine Learning and Deep Learning in Cybersecurity • Ethical Hacking & Penetration Testing or equivalent knowledge, skills and competencies acquired through prior study or professional experience.
Malware Analysis	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.
Law, Compliance, Governance, Policy, and Ethics	Basic understanding of cybersecurity principles, computer networks, and foundational knowledge of legal frameworks.
Security Operations	Basic understanding of networking and operating systems (Windows & Linux), familiarity with cybersecurity principles, and knowledge of IT infrastructure. Programming/scripting skills (Python, Bash, PowerShell) are beneficial.
Technological Foundations for CS & Security Controls	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
Cybersecurity Economics & Supply Chain	Basic understanding of cybersecurity.
Cybersecurity Education & Training Delivery I	Technological Foundations for CS & Security Controls - or equivalent knowledge, skills and competencies acquired through prior study or professional experience

Cybersecurity Education & Training Delivery II	• Technological Foundations for CS & Security Controls • Cybersecurity Education and Training Delivery I or equivalent knowledge, skills and competencies acquired through prior study or professional experience
Cybersecurity in Industry - Security of OT & CPS	• 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.
Cybersecurity Law & Data Sovereignty	Basic understanding of cybersecurity principles, computer networks, and foundational knowledge of legal frameworks.
Machine and Deep Learning in Cybersecurity	• Automation of Security Tasks and Data Analytics or equivalent knowledge, skills and competencies acquired through prior study or professional experience
Digital Forensics, Chain of Custody and eDiscovery	• Law, Compliance, Governance, Policy, and Ethics or equivalent knowledge, skills and competencies acquired through prior study or professional experience
Threat Intelligence	• Familiarity with Linux distributions, Python scripting • Knowledge of C/C++, OS design is desirable
Thesis	In order to enroll, students must have completed at least two mandatory taught modules and a minimum of 30 ECTS total. Completion of the "Research Methods" module is recommended, but not mandatory.

Students who do not fully meet the stated prerequisite expectations for a module they wish to take are recommended to complete the relevant prerequisite modules in advance, as outlined in the *Module Handbook* (Annex 7). Course scheduling within the Master's programme takes these prerequisite pathways into account (Table 2), ensuring that, for each cohort, foundational modules are offered before modules that build upon them.

Table 2: List of Recommended Prerequisite Modules in the Curriculum

Prerequisite Module	Recommended for
Ethical Hacking & Penetration Testing	AI & Emerging Topics in Cybersecurity
Law, Compliance, Governance, Policy, and Ethics	Digital Forensics, Chain of Custody and eDiscovery
Research Methods	Recommended but not obligatory for "Thesis"
Security Operations	AI & Emerging Topics in Cybersecurity
Technological Foundations for CS & Security Controls	Cybersecurity Education & Training Delivery I Cybersecurity Education & Training Delivery II
Automation of Security Tasks and Data Analytics	Machine and Deep Learning in Cybersecurity
Cybersecurity Education & Training Delivery I	Cybersecurity Education & Training Delivery II
Machine and Deep Learning in Cybersecurity	AI & Emerging Topics in Cybersecurity

If preferred, you may also choose to develop prerequisite knowledge independently, making use of **self-study materials available through the Welcome Module**.

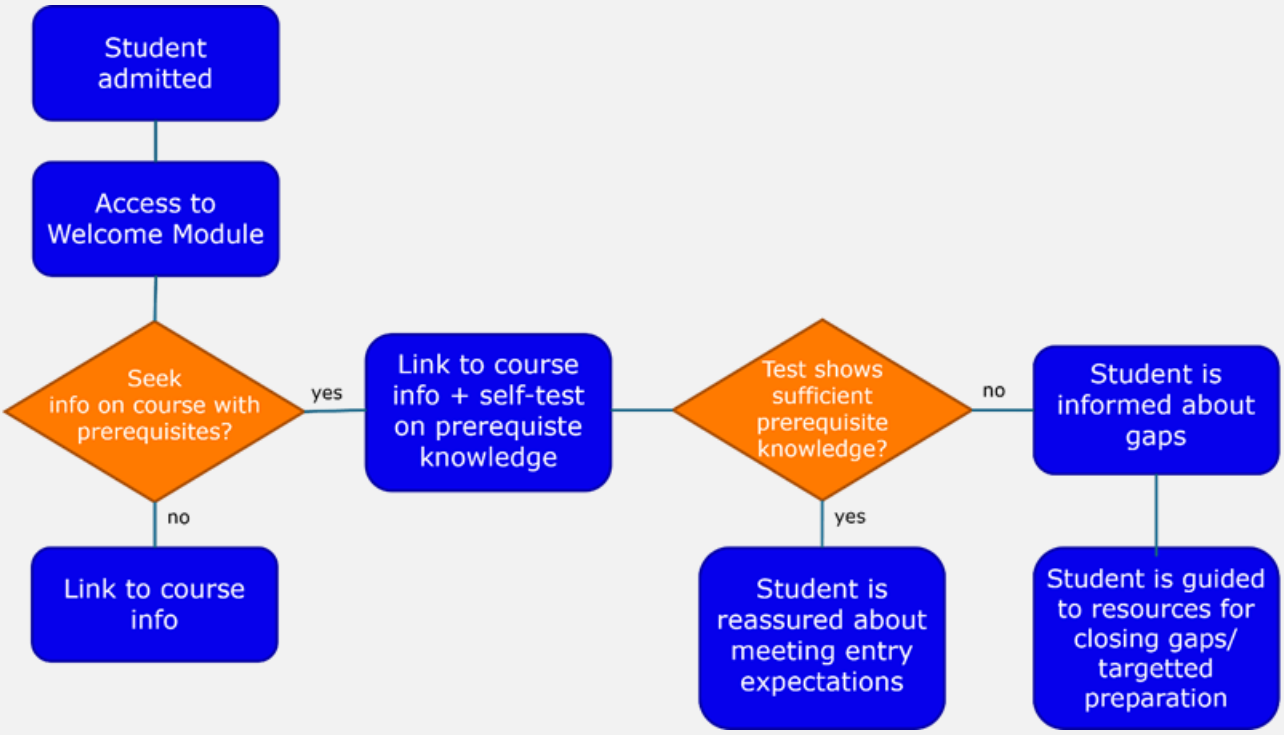
11. Support in the Welcome Module

Upon admission, you gain access to the **Welcome Module**, which serves as a central orientation hub for the programme, supporting you in making informed choices about modules and study pathways. It helps you assess how your prior knowledge aligns with module expectations, particularly where prerequisites are indicated, and assists you in identifying areas where additional preparation may be helpful.

The Welcome Module furthermore provides access to high-quality self-study resources, and highlights alternative or complementary modules that can help you build relevant foundations. Rather than prescribing a single route, it emphasises transparency, choice, and informed decision-making, empowering you to plan your studies in line with your background, learning preferences, and professional goals.

Figure 1 illustrates the student user journey for navigating module selection and progression with confidence and autonomy.

Figure 1. Student User Journey in the Welcome Module, and Resources around Module Prerequisites



Profile Orientation Meetings

In addition, each **Professional Profile Coordinator** organises a **Profile Orientation Meeting** for new cohorts at the beginning of the programme. These meetings introduce the focus of the profile, provide guidance on selecting from the recommended modules, and outline typical learning trajectories. Coordinators also share outlooks on relevant **industry certifications** that align with the profile's focus and the learning outcomes of recommended modules.

Information about these meetings is communicated by email to all students registered for the respective profile. Public announcements and access details (for example, for students who are interested but not formally enrolled in a profile) are also shared via the **Announcements section of the Welcome Module**.

12. Further Support and Contact Points

If you still have questions after reading this guide, additional support is available through the following channels:

Before admission
For any questions prior to enrolment, please contact:
✉ **studyaffairs@digital4security.eu**

After enrolment – Professional Pathways
As an enrolled student, you may contact the Programme Coordinator responsible for your chosen professional profile, or a profile of interest:

- **Chief Information Security Officer (CISO)**
  Programme Coordinator – UDS
  ✉ **coordinator.uds@digital4security.eu**
- **Cybersecurity Educator**
  Programme Coordinator – UDS
  ✉ **coordinator.uds@digital4security.eu**
- **Cyber Legal, Policy, and Compliance Officer**
  Programme Coordinator – MTU
  ✉ **coordinator.mtu@digital4security.eu**
- **Cybersecurity Risk Manager**
  Programme Coordinator – MTU
  ✉ **coordinator.mtu@digital4security.eu**
- **Cyber Threat Intelligence Specialist**
  Programme Coordinator – UNIR
  ✉ **coordinator.unir@digital4security.eu**
- **Cybersecurity Auditor**
  Programme Coordinator – UNIR
  ✉ **coordinator.unir@digital4security.eu**

Technical support

For technical issues related to system access or module selection, please contact:

it@digital4security.eu

Suggestions and quality enhancement

If you have ideas for additional guidance on professional pathways or module selection that are not yet covered by the programme, you are welcome to share them with the Quality Service Committee at:

quality.committee@digital4security.eu

Document Governance

This **Guide to Module and Pathway Selection** is governed by the Quality Service Committee.

Correspondence regarding proposed changes shall be addressed to **quality.committee@digital4security.eu**, with **secretariat@digital4security.eu** copied in Cc. The Secretariat supports monitoring the full set of programme documents to ensure consistency and the maintenance of programme-wide standards.

This Guide functions as an adjunct to the *Student Handbook* (Annex 7). While the *Student Handbook* serves as the primary source of general guidance through overviews and introductory information, the present Guide provides more detailed and practice-oriented direction specifically focused on module and pathway selection. It is intended in particular to support prospective and newly enrolled students at an early stage of their studies, when direct interaction with teaching staff may not yet be available.

The Quality Service Committee holds responsibility for this document, including content and instructional design. Particular attention shall be devoted to sections that provide indicative effort estimates for modules and professional profiles in relation to students' prior backgrounds. As part of its regular remit, the Committee analyses course progression data and student feedback in order to empirically refine these estimates and present them in a way that offers meaningful orientation and decision support for students.

In addition, the Quality Service Committee shall liaise with the Master's Board, particularly with regard to regulatory matters such as rules on module and professional profile re-registration. The Secretariat shall provide support to ensure coherence across programme documentation, especially where relevant updates might be made to the *Study and Examination Regulations* (Annex 2) or the *Student Handbook* (Annex 7).

Whenever the Quality Service Committee releases a new version of this *Guide to Module and Pathway Selection*, the new document shall be shared with the Secretariat without undue delay. The Secretariat shall ensure that up-to-date information is made available through the programme's designated publication channels, replacing any outdated materials as necessary within two weeks of notification.

The current document is designated as *Professional Profile Roadmaps: A Guide to Module and Pathway Selection, Version 1 (V1)*. Editorial changes, such as spelling corrections, do not affect the version number. Version numbering remains unchanged until student agreements have been signed. Upon official publication, each version shall be dated.

Document Context and Publication

This **Guide to Module and Pathway Selection** forms part of a comprehensive set of materials that introduce, govern, and support the **60 ECTS Online Master's in Cybersecurity Management and Data Sovereignty**, a fully online joint programme coordinated and delivered by the following three higher education institutions:

- German University of Digital Science (UDS) – Coordinator
  Marlene-Dietrich-Allee 14, 14482 Potsdam, Germany
- Munster Technological University (MTU)
  Rossa Avenue, Bishopstown, Cork T12 P928, Ireland
- Universidad Internacional de La Rioja (UNIR)
  Avenida de la Paz 137, 26006 Logroño, Spain

The programme's structure, academic standards, quality assurance mechanisms, and operational procedures are described across the following documentation package:

Self-Assessment Report - a reference document for external evaluation and accreditation under the European Approach for Quality Assurance of Joint Programmes

I. Governance and Quality Assurance

- Annex 1. Cooperation Agreement
- Annex 2. Study and Examination Regulations
- Annex 3. Rules of Procedure for the Master's Board
- Annex 4. Internal Quality Handbook
- Annex 5. Programme Survey Scales
- Annex 6. Industry Advisory Board Manual

II. Curriculum, Learning and Teaching Staff

- Annex 7. Module Handbook

- Annex 8. Student Handbook
- Annex 9. Teaching Staff CVs
- Annex 10. Practical Guide for Lecturers

III. Certification and Recognition

- Annex 11. Sample Degree Certificate
- Annex 12. Sample Diploma Supplement

IV. Administrative and Operational Documents

- Annex 13. Sample Student Agreement
- Annex 14. Sample Supporting Partner Contract
- Annex 15. Sample Remuneration Manual

The programme documentation is maintained as follows:

- **SharePoint** serves as the repository for all programme documents.
- The **Welcome Module** publishes most programme documents (except those requiring protection against forgery or containing confidential information), ensuring transparency for enrolled students and staff.
- The **Digital4Security website** provides open access to selected information for prospective students and other interested parties, including admission requirements and procedures, the course catalogue, examination and assessment regulations, and other key programme details.

No.	Document	SharePoint	Welcome Module	Website
0	Self-Assessment Report	✓	✓	
1	Cooperation Agreement	✓	✓	
2	Study and Examination Regulations	✓	✓	✓
3	Rules of Procedure for the Master's Board	✓	✓	
4	Internal Quality Handbook	✓	✓	✓
5	Programme Survey Scales	✓	✓	

No.	Document	SharePoint	Welcome Module	Website
6	Industry Advisory Board Manual	✓	✓	(✓)
7	Module Handbook	✓	✓	(✓)
8	Student Handbook	✓	✓	✓
9	Teaching Staff CVs	✓	✓	
10	Practical Guide for Lecturers	✓	✓	
11	Sample Degree Certificate	✓		
12	Sample Diploma Supplement	✓		
13	Sample Student Agreement	✓	✓	
14	Sample Supporting Partner Contract	✓		
15	Sample Remuneration Manual	✓		
16	Guide to Module and Pathway Selection	✓	✓	✓

In the event of inconsistencies or conflicting interpretations among these documents, the following **order of precedence** applies:

1. Cooperation Agreement
2. Study and Examination Regulations
3. Rules of Procedure for the Master's Board
4. Internal Quality Handbook
5. Module Handbook
6. Student Handbook
7. Student Agreement
7. Programme Survey Scales
8. Supporting Partner Contracts
9. Other supporting documents

This hierarchy, as officially defined in the *Cooperation Agreement*, serves to ensure that foundational arrangements and formally adopted regulations take precedence over illustrative or operational materials.

Should the reader become aware of, or suspect, any inconsistency or misalignment between the documents, please contact secretariat@digital4security.eu.

Together, these materials form the backbone of a transformative joint programme that seeks to integrate academic excellence, industry relevance, and social responsibility. It reflects the shared commitment of academic leaders, instructors, students, industry experts, and partner institutions, to shaping a student-centred, accessible, and future-oriented study environment.

This collective effort supports:

- **Empowering cybersecurity leaders** with the capacity to anticipate and manage risks, while collaborating effectively across stakeholders;
- **Delivering high-quality, flexible online learning** grounded in real-world application;
- **Supporting lifelong learning and workforce adaptability** in a rapidly evolving digital landscape;
- **Aligning education with industry and market needs** to ensure professional relevance;
- **Facilitating European strategic autonomy** through digital sovereignty and resilient infrastructure;
- **Advancing inclusion, accessibility, and gender equality** in the cybersecurity field; and
- **Promoting responsible innovation, ethics, and regulatory compliance** in all aspects of digital security.

We thank all contributors for their continued collaboration in advancing the Digital4Security vision: to empower learners, institutions, and societies in shaping a more secure, inclusive, and sovereign digital future.

Legal Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HaDEA). Neither the European Union nor the granting authority can be held responsible for them.

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