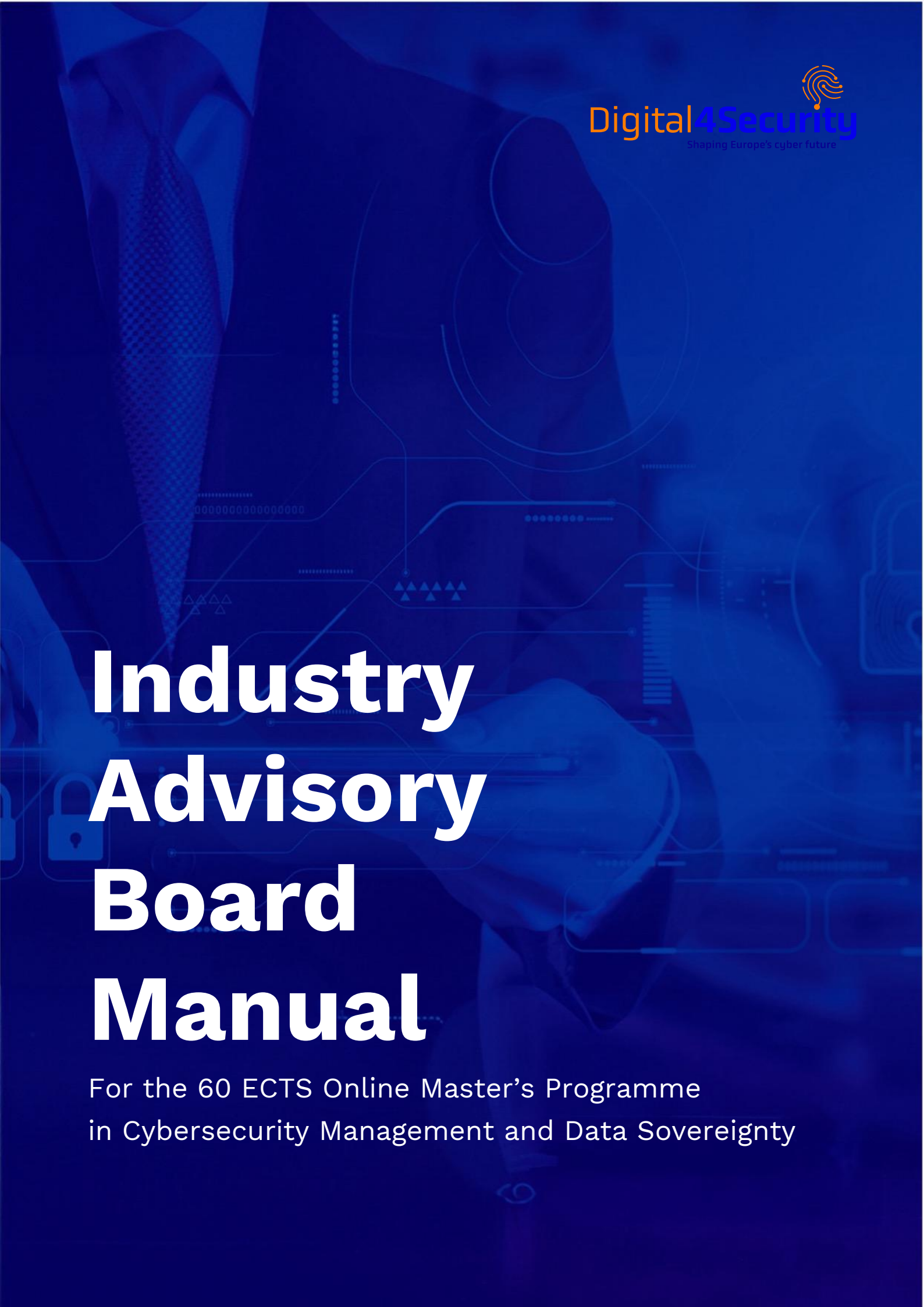


Digital4Security
Shaping Europe's cyber future

Industry Advisory Board Manual

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

Table of Contents

Preamble: Context of the Digital4Security Project

The **Digital4Security** **(D4S)** project is a strategic, EU co-funded initiative designed to address one of Europe's most pressing workforce challenges: the shortage of skilled cybersecurity professionals equipped to lead in increasingly complex digital environments. Through a close collaboration of Higher Education Institutions (HEIs), research centres, employment services, and industry stakeholders, D4S supports the co-design and delivery of high-impact, flexible education in **Cybersecurity Management and Data Sovereignty**.

At the heart of this initiative is a comprehensive ecosystem of stakeholders, united by a shared goal: to co-create education that is relevant, applied, and responsive to current and emerging needs in the cybersecurity landscape. This ecosystem has led to the development of two European Master's Programmes (a 60 ECTS online programme and a 120 ECTS hybrid programme), a growing suite of stackable microcredentials, and a pan-European knowledge and collaboration infrastructure. These offerings directly support digital upskilling, reskilling, and professionalisation across a diverse learner audience.

The **Industry Advisory Board (IAB)** plays a pivotal role in realising the D4S mission. By bringing together expert representatives from partner companies, associations, and industry-focused organisations, the IAB ensures that the educational offerings remain aligned with current labour market trends, regulatory requirements, and emerging technological developments. The IAB also strengthens ties between academia and industry, facilitating mentoring opportunities, providing feedback on course content, supporting project-based learning, and helping to validate the employability of graduates.

This Manual underpins the IAB's engagement, roles, and responsibilities in relation to the Digital4Security project. Having been shaped in an extended process of collaboration and joint revision, the Manual is also a working document insofar as the IAB can make adjustments over time, in a self-governing manner.

The content of this Manual has been set forth to govern the IAB's activities and support for all D4S educational products, including:

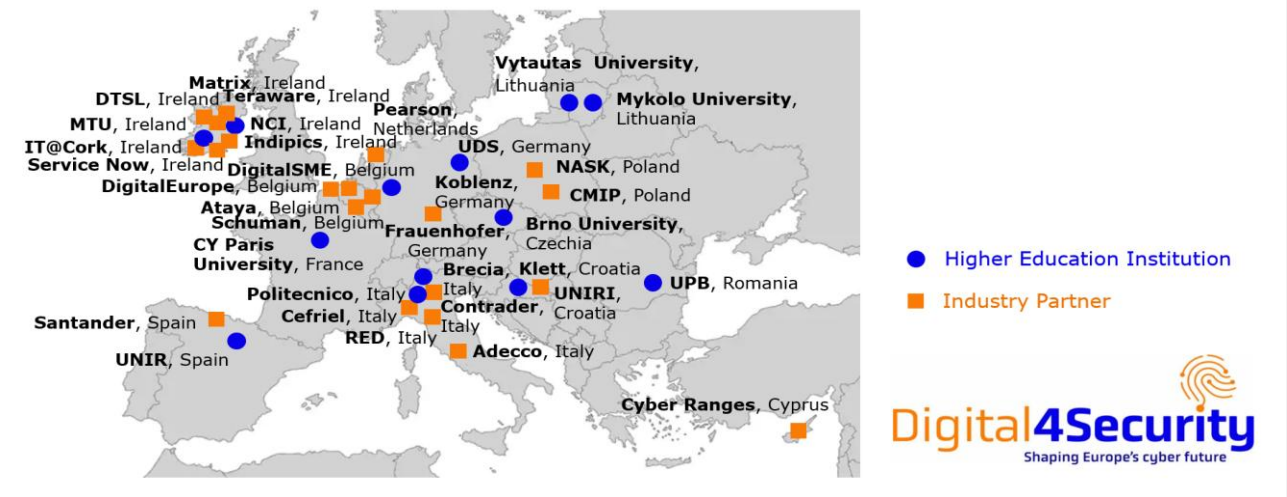
- The **60 ECTS Online Master's Programme** in Cybersecurity Management and Data Sovereignty, designed for experienced professionals, coordinated by the German University of Digital Science (UDS), in collaboration with Munster Technological University (MTU) and Universidad Internacional de La Rioja (UNIR);
- A **120 ECTS Hybrid Master's Programme**, led by the University of Bucharest and partners;
- A growing portfolio of **microcredentials** developed across the D4S network.

While all industry-affiliated organisations formally associated with the D4S project are automatically considered members of the IAB, their specific forms of engagement – ranging from curriculum review to guest lectures or mentorship – may vary, with options for engagement further described in this Manual.

The ongoing relevance and success of the Digital4Security programmes depend on the active, insightful, and forward-looking contributions of industry partners. Through continuous involvement and collaboration, the IAB ensures that graduates of these programmes are not only academically qualified, but also job-ready and equipped to take on key cybersecurity leadership roles, including Chief Information Security Officer (CISO), Cybersecurity Risk Manager, Cyber Threat Intelligence Specialist, and more.

Together, the Industry Advisory Board and academic institutions uphold the dual goals of educational excellence and practical relevance, ensuring that Europe continues to build resilience in the face of complex cyber challenges. Figure 1 illustrates the broad Digital4Security partner network realising this vision.

Figure 1: The Digital4Security Network of Partners across Europe.



This Manual serves as a practical guide to the IAB's structure, expectations, engagement formats, and contribution opportunities – particularly in relation to the 60 ECTS Online Master's Programme. It is both a reference and a framework for collaboration, enabling industry partners to contribute meaningfully to a programme that directly shapes Europe's cybersecurity future.

This Manual is intended as a **Master Document**. It presents the content developed for the IAB's role across all Digital4Security (D4S) educational offerings. However, now integrated into the governance documents of the 60 ECTS Online Master's Programme, it is specifically tied to this product. Given that the Online Master's represents the main output and flagship product of the EU co-funded Digital4Security project, it is recommended that any changes the IAB wishes to introduce be documented in this Manual. By following this approach, the document can also serve as a blueprint for IAB engagement in other D4S offerings, including the hybrid master's programme and micro-credentials.

1. Introduction

The role of industry partners and the Industry Advisory Board (IAB) was initially described and regulated in the Digital4Security (D4S) **Grant Agreement**.

Section 2 provides an overview of the IAB's role and strategic value within the Digital4Security programme, forming the basis for collaborative innovation in cybersecurity education.

Section 3 includes excerpts from the D4S Grant Agreement, offering background information as well as initial definitions and role descriptions.

Section 4 presents an IAB Charter, which may be adapted over time in a self-governing manner by the IAB.

Section 5 lists the eligible institutions from the D4S Consortium and the current nominations for IAB representatives and spokespersons. Any relevant information or opportunities concerning industry partners and the IAB may be shared directly via the contact details provided.

The **Document Context and Hierarchy Overview** explains how the Industry Adisory Board Manual relates to other key documents of the 60 ECTS Online Master's Programme.

The **60 ECTS Contacts** provide an overview of the Master's programme governance structure with contact details.

Appendix A provides a tabular overview of key IAB tasks and responsible parties.

2. Role of the Industry Advisory Board (IAB)

The **Industry Advisory Board (IAB)** is a cornerstone for fostering close collaboration between academia and industry within the DIGITAL4Security programme. It provides industry partners with a unique platform to actively shape the future of cybersecurity education and talent development in Europe, ensuring that the sector's specific cybersecurity needs are effectively addressed. Membership offers access to valuable resources, partnerships, and a pipeline of highly skilled talent.

Once it becomes operational in a self-governing manner, the IAB can evolve into a publicly visible entity, showcasing its members' close collaboration with academia and other industry stakeholders. This visibility highlights the members' active role in staying at the forefront of cybersecurity developments across Europe.

While IAB leadership roles carry specific responsibilities, and the EU Grant Agreement imposes its own regulations, general membership in the IAB is designed to be flexible. Members receive information, invitations to meetings, voting rights, access to tools and resources, and the opportunity to submit proposals. Initially, membership does not impose obligations, such as mandatory attendance or curriculum reviews. However, if the IAB faces organizational challenges – such as insufficient volunteer feedback on curriculum quality – it may adopt measures to ensure active contributions balance the benefits of membership.

KEY FUNCTIONS OF THE INDUSTRY ADVISORY BOARD (IAB)

1. Strategic Guidance for Academic Excellence

- **Strategic Influence on Curriculum Design**
  Members play a pivotal role in helping to develop a market-driven curriculum that reflects the ever-evolving cybersecurity landscape. This ensures

the programme remains relevant to current and future industry challenges in Europe.

- **External Quality Control**
  The IAB operates independently from the Higher Education Institutions (HEIs) that offer the Master's Programme in Cybersecurity Management and Data Sovereignty. Members of HEIs with academic responsibility for the programme are not eligible for IAB membership. This independence enables the IAB to conduct annual external quality reviews, acting as an impartial corrective to academic strategies.

2. Integration of Industry Expertise into Education

- **Programme Activities**
  Members can contribute to the programme through guest lectures, hackathons, weekend workshops, and hybrid events. These activities inject real-world expertise into the classroom while fostering deeper student engagement.
- **Project Opportunities**
  Members can involve students in internships, project challenges, and thesis topics to address real organizational objectives. These collaborations provide fresh perspectives and practical solutions to participating organizations.

3. Talent Development and Recruitment

- **Direct Engagement with Future Talent**
  Members gain access to top-tier students via internships, mentorship programs, and collaborative projects. These initiatives create a seamless recruitment pipeline of graduates with industry-relevant skills and certifications.
- **Certification and Skills Development**
  Members can shape certification pathways to meet sector-specific needs, while also benefiting from tailored short courses designed to upskill their workforce.

4. Research and Innovation

- **Access to Research and Innovation**
  Industry partners benefit from early access to cutting-edge research, innovative tools, and methodologies. Sector-specific case studies offer actionable insights.

ACCESS AND ENGAGEMENT OPPORTUNITIES

1. Events and Networking

- **Participation in Tailored Events**
  Members can host and attend workshops, networking events, and guest lectures focused on sector-specific challenges and emerging technologies.
- **Networking and Collaboration**
  The IAB connects members with a pan-European ecosystem, including HEIs, training providers, cybersecurity clusters, SMEs, and EU Commission representatives.

2. Digital Tools for Collaboration

- **Digital Learning and Matchmaking Tools**
  Members can contribute content, mentor students, and access resources through the programme's online platform, enabling real-time collaboration with faculty and learners.

3. Insights for Strategic Decisions

- **Data-Driven Market Insights**
  Members receive insights into market trends and skills gaps via annual surveys, interviews, and research reports, empowering informed, data-driven decisions.

3. Grant Agreement: Sections on the Role and Involvement of Industry Partners

The following sections from the D4S Grant Agreement provide insights into the original idea and mission of the Industry Advisory Board (IAB) within the context of the European Master's Programme in Cybersecurity Management and Data Sovereignty. These ideas may also serve as a guide, or point of reference, in the IAB's subsequent self-governance.

Quotes in this Manual refer to the Multi-Beneficiary Grant Agreement with the European Health and Digital Executive Agency (HADEA) under the Digital Europe Programme, concerning funding for Project 101123430: Digital4Security.

In an editorial capacity, bold print has been adjusted within quoted text to emphasize key terms and core concepts relevant to the role of industry partners in the Digital4Security project. Additionally, two typographical errors found in the original Grant Agreement have been corrected, each involving the removal of a surplus letter.

"Our Digital4Security **Programme will be market and industry demand-led** at its core, continuously adapting and evolving to address current and future cybersecurity risks and supporting European companies, and in particular SMEs, to minimize security risks, build robust defences, and effectively manage any cyber incident." (p. 10)

"Develop a dynamic pan-European Cybersecurity stakeholder ecosystem where HEIs, Industry partners, Training providers and Cybersecurity clusters **work together to design, promote, deliver and improve an innovative Cybersecurity Management Programme** that will be developed and delivered by the best cybersecurity talent from Europe and Worldwide." (p. 80)

"Establish an **Industry Advisory Board led by** [...] **key industry stakeholders**. Education and industry stakeholders will be **recruited** into the partnership as Associated Partners **on an annual basis** by invitation of consortium members, aligned with the Partnership Development Strategy in WP5 (12 new HEIs and 24 new Industry Partners by M48.) Programme of **Online and Offline Meetings to coordinate the project and strengthen the partnership**. **1 x Physical Partners Meeting per year** [...] **and 5 bi-monthly Online Partners Meetings per year**, 24 Partner Meetings in total by M48." (p. 80)

"Market Needs Analysis to identify existing and emerging Cybersecurity **skills needs among companies, SMEs and Start Ups** that need to be addressed by the programme. This will include a combination of desk research into existing reports and studies along with **surveys and interviews among companies, facilitated by the industry partners** and training providers. The Needs Analysis report will also define the ECSF Occupational Profiles that the programme will be focused on." (p. 81)

"Utilise the Industry Advisory Board to join and participate in the design phase, ensuring a **programme tailored to the needs of the market**, as well as the **engagement of private companies in the delivery of the Masters**." (p. 81)

"Define the requirements for a common online learning platform, which would also include **content from industry partners**." (p. 81)

"**Industry Certification pathways**" (p. 81)

"Design the **programme** of weekend workshops, guest lectures, networking events, cyber challenges, capture the flag exercises, projects, hackathons etc. throughout the Masters programme, **hosted by each HEI & Industry Partners**" (p. 81f.)

"A sophisticated Train-The-Trainer programme for faculty will support the quick adoption of the **platform for lecturers** from within each of the 12 HEIs and other guest lecturers or **experts from academia or industry**." (p. 83)

"T4.3 Student Mentoring and Support by Industry Experts
Student mentoring & support by senior experts selected from Industry Advisory board, industry partners from the consortium, participating SMEs and Companies, and other leading European and International firms. **Students can select their industry mentors from a panel each year, or they can 'buddy' with the staff of participating companies to get involved in joint projects / cybersecurity challenges and gain more real-world experience**. The Digital Learning **Platform will provide a matchmaking tool to allow industry experts from the consortium and participating companies to post their interest in being involved, and for students to review the panel and request suitable experts**. The consortium **industry partners will ensure a comprehensive panel** of cybersecurity management experts is available to support each student during each intake" (p. 84f.).

"T4.4 Weekend Workshops, Networking Events and Guest Lectures
Series of Weekend Workshops, Networking Events with Guest Lectures to bring together the students, faculty, experts and companies participating in D4S at regular events. The events will include digital skills experts and business leaders presenting **real case studies from industry** and talks on specialist cybersecurity management and technical subjects, along with other **interactive workshops, projects and team activities**. We will schedule 3 physical events per semester open to all students across the active courses, hosted by different HEIs, totalling 6 per year or 18 in total. The events will be designed to be hybrid, enabling large scale participation for all students even if they can't travel. The format of each **event will be linked to a specific technology area or hot topic** that will ensure maximum interest and engagement. Each HEI and **Industry partner has been allocated a budget to host or contribute to the set up and running of at least one event**, ensuring a very diverse programme." (p. 85)

"T4.6 Industry Certifications & Micro-Credentials
A key part of the programme delivery will be the **Industry Certifications provided to students by a Certiport Certification partner in their country**. Flexible test centres for remote and in-person examinations will be set up under WP3 and used to provide the testing in close cooperation with each national HEI. **Micro-credentials**

/ degrees will also be provided for individual modules and courses, allowing students to build a portfolio of certifications throughout their 2 or 3 year studies and significantly increasing job prospects." (p. 85)

"T4.7 Short Courses, Work Based Learning and Employability Programme
Prepare a series of Short Courses for SMEs and companies with certification, including individual modules from the Masters programmes with micro-credentials for each module and certification for the short course. The courses are designed for business managers / leaders as an introduction to the topics of the Masters and are **tailored to specific sectors**. We aim to provide **training to min 900 SMEs/Companies from different sectors** and across multiple countries. In Ireland and Italy direct training will be provided to a larger cohort of companies to develop a best practice approach for future phases. The HEIs and **industry partners will also host and run smaller training programmes in their respective countries**. We also aim to **train a min 1200 staff in companies via online modules** with micro credentials by M48. Deploy a **Work-based Learning** component that supports both students and host companies / SMEs. Implementation of an Employability Programme for **students who wish to find a new position in a company** after the Masters and require '**match making**' **with potential employers**. We aim to place **min 1500 students into job placements / internships.**" (p. 86)

"The launch campaign will also **target SMEs and industry players to encourage them to enrol their staff in the programme and participate in the employability programme, weekend events, collaborative projects and student support activities**" (p. 87)

"a **partnership development strategy** (including an MoC) to build a pan-European ecosystem of Industry and Education partners, strengthening the network of content contributors, industry experts, and host companies year on year. New partners will join as Associated Partners of the programme and be involved in its activities (e.g., host career talks, weekend workshops, take part in the employability programme, pilot the D4S programme, etc.)." (p. 88)

"**surveys and interviews with industry partners, host companies**, and students to determine **how effective the project has been** at strengthening competitiveness, delivering benefits for society, offering a career path and increasing cybersecurity awareness and skills. (p. 88)

"develop and implement an EU-wide communications campaign to promote the results and outputs of the DIGITAL4Security programme. [...] A series of events/webinars (at least 8) will be organised in close collaboration with partners to present the key outputs and results, case studies collected (T5.6) and **empower industry and education stakeholders to use the D4S results**. For these events, countries with lower level of advanced digital skills/cybersecurity skills (DESI 2022) will be prioritised." (p. 88)

"Developing a sustainable Masters programme with industry certification and EU accreditation that align with the needs of industry employers and other HEI and training providers. The **programme will be designed and reviewed in collaboration with the Industry Advisory Board to ensure it remains relevant to fit changing industry needs**. [...] We will also select available industry certifications that align with modules and offer industry recognised certs. 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**." (p. 89)

"We also have a large pool of **specialist cybersecurity experts** within our consortium, from both academia and **industry**, who will be utilised **as lecturers, mentors and project leaders for both the academic courses and onsite / hybrid events and cyber challenges**." (p. 115)

"Another key aim of our consortium is to create a **European Stakeholder Network** where Academia, Industry, Research, and Employment work together to design,

deliver, promote and improve a Masters Programme that will create highly employable Cybersecurity talent. We will provide Capacity Building and Training for the Universities & Training Organisations delivering the programme, building on their strengths and sharing resources, helping them recruit top teaching staff and leading experts from both the consortium and other industry and academic partners, and building **strong and long-lasting connections between Cybersecurity academia and industry**. **The central pillar of our programme will be the involvement of European companies and SMEs from multiple sectors in the design and delivery of the Masters, and throughout the programme we will provide practical support that will help them to identify their cybersecurity risks and skills gaps and then retrain existing staff or recruit new talent via the Masters Programme**." (p. 115)

"We will adopt a flexible & tailored approach to the programme design and delivery to **cover any industry** as needed. The Masters programme itself will be adaptable to accommodate different student personas and career pathways across sectors, and we will also develop a complementary **portfolio of short courses and individual modules tailored for specific industries**. We understand that in certain industries and company types there are no specific or dedicated roles for cybersecurity professionals, and therefore we will leave it open **for companies who wish to upskill or retrain their team with additional cybersecurity management skills to complement existing job profiles**" (p. 115f.)

"The programme will **blend academic and industry content** to ensure that graduates are equipped with both theoretical and **job-ready cyber skills to fast-track employment**. [...] **New content will be developed collaboratively between industry and educational partners to meet the specific needs of companies.**" (p. 116)

"Being a market-oriented study programme, DIGITAL4Security will be designed to **meet the needs of industry with training, qualifications, certification and practical experience** that will help them address their cybersecurity skills gaps. [...] The 120 ECTS-CPs will be achieved via a **mix of online modules, collaborative projects, and cybersecurity challenges**; with optional weekend workshops, networking events, and physical meet ups hosted by the HEIs and Industry Partners in each

country [...]. The **programme will be delivered by** some of the leading researchers, experienced lecturers, and **industry experts from the cybersecurity sector** in Europe, most of which will be drawn from our large consortium of academic, training, research and industry partners." (p. 117)

"The **courses will blend academic and industry content** to equip graduates with theoretical and job-ready digital skills to ensure they will be successful on the job market and highly effective in their new roles. Their Masters will [...] comprise industry certification [...] to guarantee that they have mastered critical aspects of their course and are fully 'market ready'. The **course content will include ready to use online learning modules from** [...] **industry and academic partners**, and the partnership includes certification subcontractors in each of the partner countries to facilitate both onsite testing in each HEI and online testing platforms. **The cost of industry certifications will be covered in the highly competitive student fees**, making it extremely attractive and accessible for the students.

"The European Masters will be delivered via one shared central digital learning **platform** (www.digital4security.eu) **containing resources from** HEIs and **Industry**, supported by physical workshops, networking events, guest lectures, bootcamps, and cybersecurity challenge-based projects. **The online platform will contain a large repository of Cybersecurity training content for students, companies and faculty**, including short courses and modules that can be taken as stand-alone training with micro credentials. Each of the academic and **industry partners will collaborate to design the central online** European Cybersecurity Masters **Programme** and **contribute to the delivery with their own content, expertise, facilities and faculty**, working together to create an innovative 'Masters-as-a-Service' platform delivery model that can be scaled up to a pan-EU level with relative ease. This approach also allows each HEI and all consortium partners to **have access to a shared Cybersecurity educational resource** that they can all use to support their students and empower their faculty. Contributing to a central European Masters also allows them to continue their own separate academic programmes without having to create and add a whole new physical academic degree. The digital learning platform will host all the educational content, course registrations, projects,

student data etc. [...] In addition, **the platform will be populated with the online learning modules and content provided by** the academic & **industry partners** and with the new material developed specifically for this programme. (p. 119)

"Integrating SMEs and larger Companies into the Programme - To ensure a **completely industry led Masters** we will integrate SMEs and companies into the design, development, deployment and dissemination of the programme. Within WP2 we will undertake a market needs analysis to define the **specific occupational profiles that need to be filled and the cyber skills, technology competences and business knowledge required by each graduate**. The needs analysis will build on the existing skills needs analysis work undertaken by ENISA and the REWIRE project, the Cybersecurity Skills Alliance funded by Erasmus+. (Several [of] our consortium members are involved in REWIRE). SMEs and companies will be recruited as partners from the very start and encouraged to help to co-create a programme that will **address their real commercial needs**. **During the programme design and delivery stages companies will be invited to contribute industry experts as part of an Industry Advisory Board, provide staff to present as guest lecturers / workshop panellists, set real life challenges that will address their needs, work with students on collaborative projects to create solutions, and participate in events such as cybersecurity challenges in cyber ranges**. To support the employability and lifelong learning of graduates we will also provide ongoing access to online learning content to facilitate continuous work-based learning when in employment, **match making of students and companies via pitching events and networking**, an alumni network to provide networking and support to current and past students, and the provision of micro-degrees / credentials and industry certification that ensures they are fully qualified and **aligned with the specific skills and tools the companies need**. **SMEs and companies engaged in the programme will also be encouraged to participate in dissemination activities and promote the project outputs and their involvement in activities via their own channels**. We will also encourage and support the alignment of their DIGITAL4Security participation with support provided by the European Digital Innovation Hub network. In addition, we will also **design and deliver specific short courses for SMEs and companies**

and create specific events to engage and educate teams from companies of all sizes." (p. 119)

"**DIGITAL4Security will also help companies to safely adopt new digital technologies and solutions to help them drastically reduce their own climate and environmental impact, as well as developing new solutions, products and platforms that will help other sectors of European industry and society to adopt new 'climate neutral' models of working, learning and living**." (p. 120)

"**Set up** Project Steering Committee, **Industry Advisory Board**, Project Management Team & Quality Assurance **processes, guidelines and measurement tools**." (p. 126)

"Curriculum review process to **update the programme based on changing industry needs and new technical enhancements**." (p. 126)

"**Student mentoring & support by senior experts selected from industry partners** and other leading firms" (p. 127)

"Develop and implement an **EU-wide communications campaign** to promote the launch of the new programme and each annual **intake of** the Masters to both students and **companies**, ensuring high student enrolment levels and industry participation." (p. 127)

"**Partnership development strategy** to build a pan-European ecosystem of Industry and Education partners, **strengthening the network of content contributors, industry experts and host companies year on year**. Design and execute an EU-wide campaign focused on promoting **D4S as a best practice to Industry** and Education providers. Develop a series of webinars and hybrid **online / offline networking events for** both Education and **Industry**, highlighting key outputs, activities and **case studies from the programme**." (p. 127)

"Industry Advisory Board (IAB)
[Key role:] Strategic guidance and quality control. Coordinated by the Project Director, **it is responsible for planning and implementing the business changes that need to be made for the organisation to effectively integrate the project deliverables into its everyday work**. [Composition:] **Domain experts from industry/academia across the core technology pillars and including representatives from the European Commission**." (p. 128)

"Industry Advisory Board[:] **To provide an additional layer of strategic guidance and quality control, we will establish an external Industry Advisory Board, inviting domain experts from industry/academia and including representatives from the EC as required**. This mechanism has been used in other projects with great success and it **provides an extra layer of external validation and leadership to the whole project**." (p. 129)

"**Industry experts and mentors can be recruited from participating companies and industry partners** at a relatively low cost and the online model also makes it very convenient and accessible for additional EU and international experts to participate if needed." (p. 130)

"In order to achieve this goal, we have assembled a veritable **'Dream Team' of Cybersecurity experts from Industry** and Academia [...]. Our consortium brings together leading higher education institutes, research & excellence centres, cybersecurity industry clusters, VET training and work-based learning providers, employment experts, certification bodies, industry representative groups, large tech companies, and specialist SMEs and start-ups." (p. 131)

[Key performance indicators:]

"Number of collaborations with industry:

- Weekend Workshops, Networking Events and Guest Lectures from digital skills experts and business leaders (3 per semester hosted by a different HEI or industry partner, min 18 in total over 4 years)

- Cybersecurity Challenges in cyber ranges, hackathons, bootcamps and practical problem-solving projects developed with companies as part of the Masters curriculum. (3 events per semester, min 18 in total)
- Webinars and hybrid online / offline networking events for both Education and Industry promoting the launch of the programme and highlighting key outputs, activities and case studies from the programme. (Min 12 in total over 4 years)
- Number of new industry partners to join the consortia as associate partners and sign cooperation agreements during the project duration. [Min 40 in M48]"

(p. 143)

"SMEs & Companies

- Number of SMEs/companies with **existing staff enrolled in D4S**.
- Number of **SMEs/Companies who participate in tailored short courses** with certificates for their industry / sector. [...]
- Number of **online modules with micro credentials completed by staff** in SMEs/Companies [...]
- Number of **graduates employed by SMEs/companies from D4S** [...]
- Number of **new job placements or internships in SMEs/companies** during studies. (Employability & Mobility Programme)"
  (p. 143)

"The **model** can be implemented **for any digital upskilling programme by any consortium of academic and industry partners**." (p. 147)

"[Beneficiaries:] **SMEs & Companies sending staff for upskilling / reskilling or participating in the programme to hire graduates**.
[Expected impacts on competitiveness:] D4S is designed to help European **companies and SMEs** to achieve long term competitiveness and growth by **directly supporting their digital transformation and innovation by helping to upskill existing staff**. It will provide trained employees to fill crucial cybersecurity profiles that

are in very high demand and are critical to the security and success of each business. **Without the programme they would not have access to these staff very easily or cost effectively, and this gives them a significant advantage over competitors.**" (p. 147)

"DIGITAL4Security will contribute to the following **UN Strategic Development Goals** within Europe: [...] 9. Industry, Innovation & Infrastructure"

4. Industry Advisory Board (IAB) Charter

The Industry Advisory Board (IAB) Charter outlined below has undergone initial review by IAB representatives. At the same time, it is intended as a living document – providing a structured foundation for the Board's self-governance, outlining key operational elements. The Charter may be revised over time by the IAB in line with its evolving priorities and self-governance procedures.

Article I: Purpose

The primary purpose of the Industry Advisory Board (IAB) for the DIGITAL4Security European Master's Programme in Cybersecurity Management and Data Sovereignty is to collaborate with Academic Partners to design, promote, deliver, and continuously improve an innovative cybersecurity management curriculum. At its core, the program is designed to be market- and industry-driven.

The IAB offers recommendations and resources to:

- Update the curriculum and expand the stakeholder network.
- Integrate emerging industry challenges, solutions, practices, and tools.
- Annually review the programme to align with evolving industry needs and technological advancements, providing external quality assurance and strategic guidance.

Article II: Governance

The IAB has the authority to establish its own governance structure. Recommended components include:

- A Steering Committee with three to seven member organizations, represented by designated individuals.

- One Executive Director, responsible for setting meeting agendas, guiding IAB activities, and ensuring effective documentation.

The IAB governance bodies and representatives collaborate closely with:

- The D4S Project Coordinator during the EU-funded phase.
- Study Programme Coordinators once the Master's programmes are operational.
- In the 60 ECTS Online Master's Programme, the Quality Service Committee (responsible for curriculum evaluation and industry alignment) provides the direct interface for the IAB. It can be contacted via **quality.committee@digital4security.eu**.

Article III: Composition of the IAB

Members

The IAB comprises Associate Partners of the Digital4Security project.

Each Associate Partner organization may:

- Nominate one or two individuals to serve as official representatives.
- Allow additional representatives to participate in IAB activities.

Representatives receive:

- Invitations to meetings and access to minutes.
- Voting rights where applicable.
- Access to the Digital4Security online platform and resources.

Membership

- **New Member Enrolment:**
  New members may join the IAB at any time during the year, provided they meet the eligibility criteria.
- **Membership Beyond Industry:**
  Representatives from the European Commission and external academic institutions are eligible to join the IAB. However, academic representatives affiliated with degree-awarding institutions participating in the Master's programmes are not eligible, ensuring that the IAB maintains impartial external quality control.
- **Membership Expansion:**
  The expansion of IAB membership beyond the network from the initial Grant Agreement is encouraged. Proposed new memberships must be formally communicated in writing to the Project Coordinator during the EU-funded phase or to the Study Programme Coordinators thereafter, at least one month in advance. The Project Coordinator or Programme Coordinators retain the right to object to new memberships if a valid reason is provided.

Terms of Office

- Membership is indefinite unless an institution withdraws, ceases to exist, or is excluded by the IAB, the Project Coordinator or the Programme Coordinator.
- Representatives serve until they resign, retire, or leave their organization, ideally nominating successors.

Article IV: Rights of IAB Members

IAB members are entitled to:

- **Propose Content:** Recommend updates or additions to the Master's programmes, including workshops, lectures, events, and certifications.
- **Participate in Delivery:** Serve as lecturers, mentors, or project leaders, subject to academic accreditation requirements.
- **Access Resources:** Use Train-the-Trainer materials, online platforms, and a repository of cybersecurity training content.
- **Collaborate on Projects:** Suggest real-world challenges for student projects, including master's theses, internships, and hackathons.
- **Shape Certification Offerings:** Propose industry certifications, micro-degrees, and short courses tailored to specific sectors.
- **Promote Networking:** Leverage the IAB network to connect with cybersecurity talent, academic and industry experts.
- **Utilize Results:** Disseminate project findings and integrate them into their organizational strategies.

Article V: Tasks and Activities of the IAB

1. Strategic Advice

The IAB provides recommendations on:

- Programme evolution and alignment with industry trends.
- Addressing emerging challenges and opportunities in cybersecurity.

2. Quality Assurance

The IAB ensures programme relevance by:

- Reviewing the curriculum including each module annually. Offering feedback on educational content development.
- Participating in surveys, interviews, or external assessments.

3. Event and Content Contributions

The IAB contributes by:

- Organizing and participating in events like hackathons, cyber challenges, and networking sessions.
- Facilitating access to resources for ongoing skills development.

4. Identifying Skill Gaps

The IAB helps bridge gaps between current programme offerings and the evolving needs of European industries by issuing targeted recommendations.

Article VI: Amendment and Review

The IAB charter is a living document, subject to ongoing review and revision based on feedback from IAB members, academic partners, and external stakeholders.

5. Eligible Partner Institutions

Table 1 presents a current list of Associate Partners from the D4S Consortium. Each partner is invited to nominate one or two individuals to serve as the institution's representative and spokesperson in the Industry Advisory Board. While additional representatives may participate in this Board's activities, each partner is invited to identify one or two official points of contact.

Table 1: D4S Associate Partners (Alphabetically)

No.	Partner	Abbreviation	Country
1	Adecco Formazione SRL	ADECCO TRAINING	Italy
2	Adecco Italia Holding di Partecipazione e Servizi SPA	ADECCO GROUP	Italy
3	Adecco Italia	ADECCO ITALIA	Italy
4	Ataya & Partners	ATAYA	Belgium
5	Banco Santander SA	BANCO SANTANDER	Spain
6	Cefriel Società Consortile a Responsabilità Limitata Società Benefit	CEFRIEL	Italy
7	CMIP (Polski Klaster Cyberbezpieczenstwa Cyber-MadeInPoland Sp. z o. o.)	CMIP	Poland
8	Contrader SRL	CONTRADER	Italy
9	Cyber Ranges Ltd	CYBER RANGES	Cyprus
10	DigitalEurope AISBL	DIGITALEUROPE	Belgium
11	Digital Technology Skills Limited	DTSL	Ireland
12	European Digital SME Alliance	DIGITAL SME	Belgium
13	Fraunhofer Gesellschaft zur Förderung [Text Wrapping Break]der Angewandten Forschung EV	FHG	Germany
14	Independent Pictures Limited	INDIEPICS	Ireland
15	IT@Cork Association Limited LBG	IT@CORK	Ireland
16	Matrix Internet Applications Limited	MATRIX	Ireland
17	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	NASK	Poland

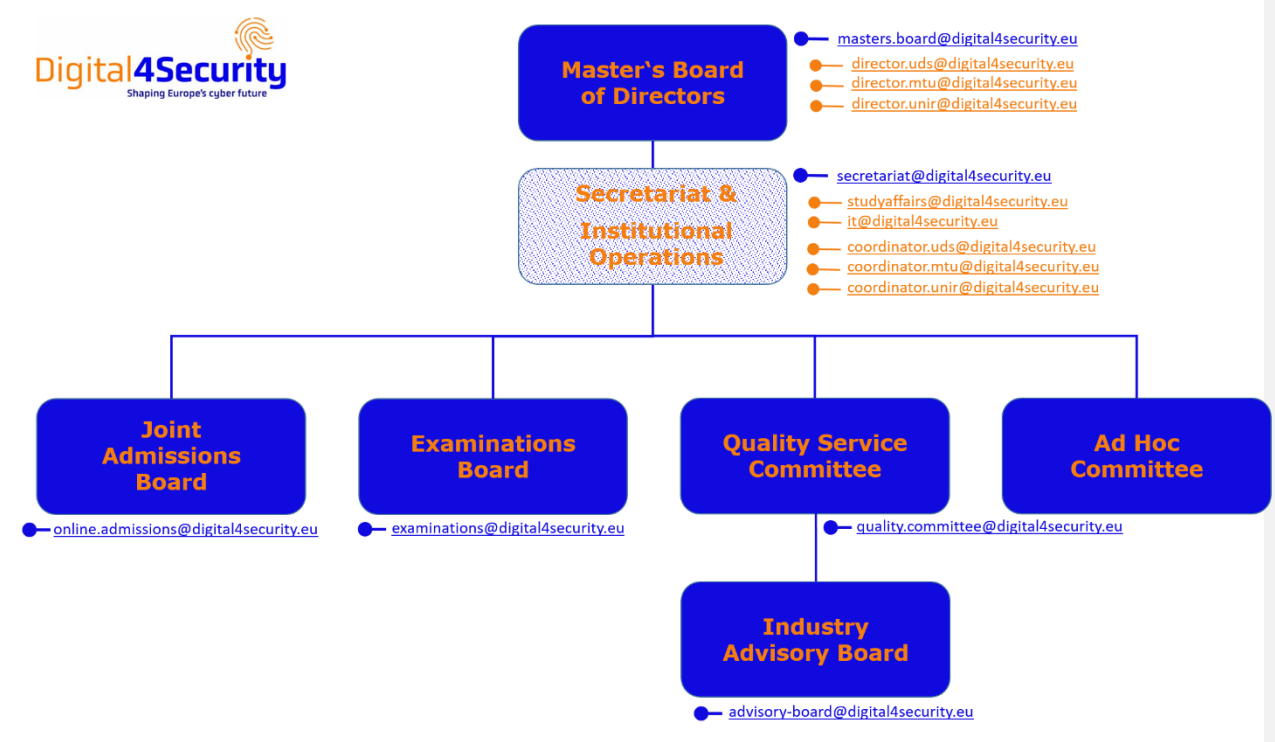
No.	Partner	Abbreviation	Country
18	Pearson Benelux	PEARSON B.	Netherlands
19	Profil Klett d.o.o.	PROFIL KLETT	Croatia
20	Red Open S.R.L.	RED OPEN S.R.L.	Italy
21	Schuman Associates SCRL	SA	Belgium
22	ServiceNow Ireland Limited	ServiceNow	Ireland
23	Skillnet Ireland Company Limited By Guarantee	SKILLNET	Ireland
24	Terawe Technologies Limited	TERAWE	Ireland

60 ECTS Programme: Governance Structure and Contacts

As the Industry Advisory Board plays a key role in reviewing the 60 ECTS Online Master's Programme and ensuring its ongoing relevance to industry needs and developments, it is important to streamline correspondence and maintain a clear overview of contact points.

The governance structure of the 60 ECTS Online Master's Programme is presented in Figure 2, along with key contact details at all levels.

Figure 2: Overall governance bodies and contacts for the 60 ECTS Online Master's.



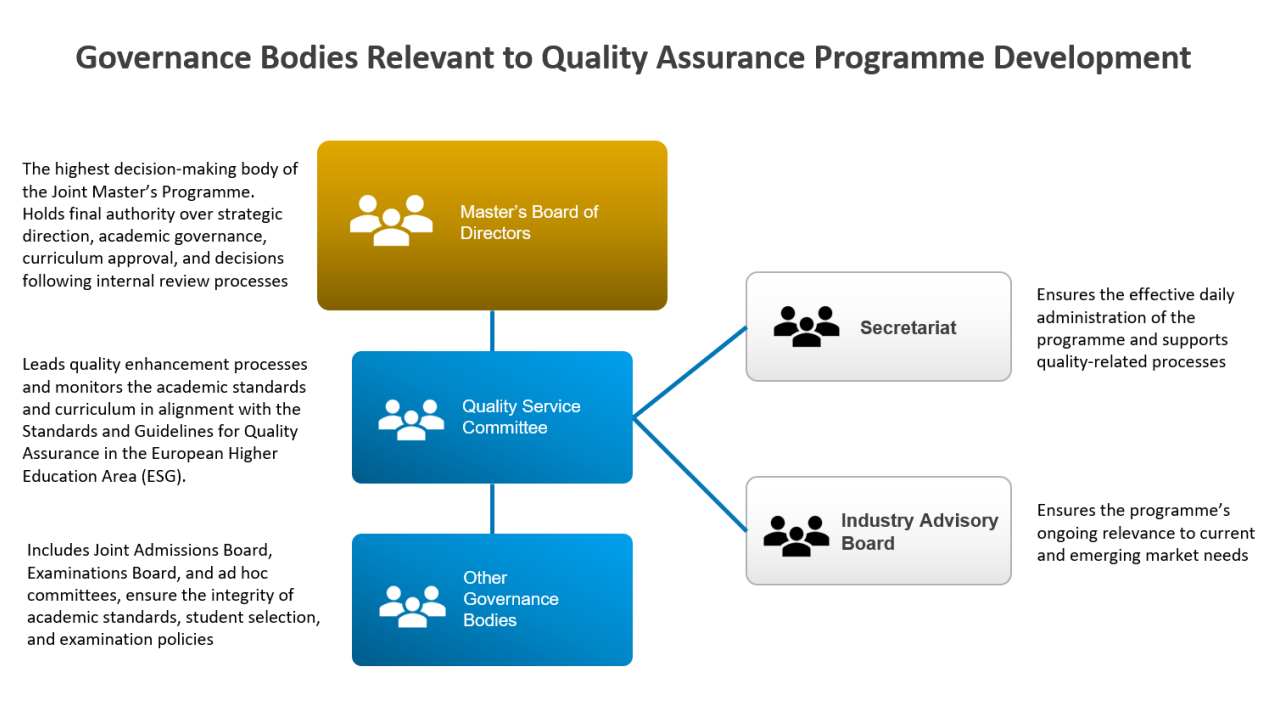
The highest decision-making authority rests with the Master's Board, which comprises the Programme Directors from the three awarding institutions, UDS, MTU, and UNIR. The Secretariat supports day-to-day operations and assists the various boards and committees.

The Industry Advisory Board operates largely independently of the Master's Board, acting as an external corrective to support continuous industry alignment. Its primary role is to provide expert insights and recommendations, particularly to the Quality Service Committee (QSC), which is the most important point of contact for the IAB.

According to the programme's Cooperation Agreement, the QSC includes up to three voting members from the Digital4Security network, ideally selected from the IAB to support streamlined exchange and close collaboration.

The governance structures specifically dedicated to quality assurance are outlined in Figure 3. In this context, IAB contributions play an essential role.

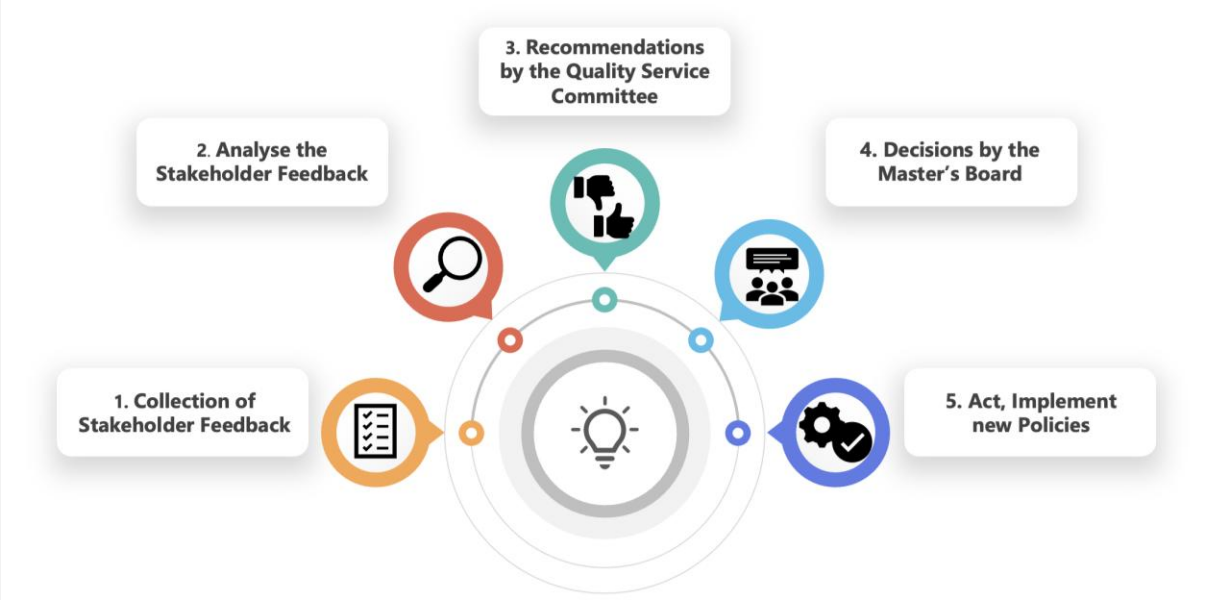
Figure 3: Governance bodies relevant to quality assurance.



The programme follows an annual quality assurance cycle, presented in Figure 4. As part of this cycle, the QSC invites module reviews by industry experts. To do

so, it contacts the IAB's Executive Director and Steering Committee, who then have three months to identify and assign two expert reviewers per module.

Figure 4: The annual quality assurance loop in the Master's programme.



Reviewers are granted access to all relevant teaching materials on the D4S platform. The module review is conducted by filling the *"Survey for Industry Experts"* from the Programme Survey Scales (Annex 5). Reviewers are given three months to answer the questionnaire.

Completed module assessments and recommendations are shared with module instructors. The QSC consolidates all input into a draft **Annual Programme Review Report**, which includes aggregate module-level data and recommendations on the programme level. Final decisions are taken by the Master's Board, and the approved report is shared with all IAB members to ensure full transparency.

Toward the end of the Spring Term, the QSC organizes the **Future of Learning Convention**, a major annual event that brings together students, faculty, programme leadership, and IAB representatives. The Convention offers an open forum to discuss findings, recommendations, and opportunities for innovation. One core

aim (alongside a student-centred study experience) is to ensure the continued industry relevance of the programme and the employability of graduates in Small and Medium-sized Enterprises (SMEs) as well as other organizations.

Document Governance

Correspondence regarding proposed changes to the IAB Manual shall be addressed to **advisory-board@digital4security.eu**. Whenever the IAB establishes a new official version of the Manual, the authorized document shall be submitted to **secretariat@digital4security.eu** within 14 calendar days to enable the update of the official programme documents.

The IAB has the authority to amend the Industry Advisory Board Charter as it deems appropriate.

Quotations from the Grant Agreement may be added if new passages with relevant information on the role or tasks of the IAB are identified. Existing quotations shall remain unchanged unless copying errors are detected, in which case corrections shall be made to ensure complete fidelity to the original source.

Descriptions of the Digital4Security project within the Manual shall only be amended if they are no longer current. In such cases, corrections may be made in consensus with the Quality Service Committee, which can be contacted via **quality.committee@digital4Security.eu**, copying **secretariat@digital4security.eu** in the Cc.

Changes to the section titled "The Role of the Industry Advisory Board" may be made at the discretion of the IAB, but must be communicated to the Master's Board at **masters.board@digital4security.eu**, with **secretariat@digital4security.eu** copied in Cc, whenever the IAB endeavours to substantially revise its key functions. In such cases, the Master's Board reserves a 14-day veto right.

The sections titled "60 ECTS Programme: Governance Structure and Contacts" and "Document Context and Publication" fall under the authority of the Master's Board and are operationally supported by the Secretariat. The IAB may not revise these sections. Any requests for updates shall be addressed to **secretariat@digital4security.eu**.

The current publication policy provides for two versions of this Manual:

- a complete version, including contact details, for internal use only; and
- a public version ("light"), excluding such details, published via the Digital4Security website.

For streamlined publication and to minimise the risk of error, the IAB may consider relocating the section containing contact details into a separate operational document. This would allow a single, unified version of the Manual to be maintained for both internal and external distribution.

The Secretariat must ensure that the section containing contact details is removed prior to making the Manual accessible on the Digital4Security website. This obligation applies to every publication and update of the document. In the present version, Section 6 ("Nominations") is marked for removal. The IAB is responsible for clearly identifying any section containing contact details for removal if such information remains part of the Manual.

The current document is designated as *Industry Advisory Board Manual, Version 1 (V1)*. Editorial changes, such as spelling corrections or updates to figures that do not alter their meaning, do not affect the version number. The version number remains unchanged until student agreements have been signed. Upon official publication, each version shall be dated.

Document Context and Publication

This **Industry Advisory Board Manual** 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	✓	✓	✓

No.	Document	SharePoint	Welcome Module	Website
5	Programme Survey Scales	✓	✓	
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	✓		

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.

Appendix – Summary of Tasks / Activities and Ownership, referencing the associated pages in the Grant Agreement

Task/Activity	Responsible Party	Page Number
Strategic guidance on curriculum evolution and alignment with industry trends	Industry Advisory Board (IAB)	14, 89
Conducting annual external quality reviews of the curriculum	IAB Members	14, 89
Participation in program activities like guest lectures, hackathons, and workshops	IAB Members and Industry Experts	14, 81, 127
Involvement in internships, project challenges, and thesis topics	IAB Members and Industry Partners	14, 81
Shaping certification pathways and providing tailored short courses	IAB Members	81, 85, 119
Hosting and attending workshops, networking events, and lectures	IAB Members	14, 85, 127
Contributing to surveys, interviews, and external assessments	IAB Members	88, 89
Supporting the design and delivery of the Master's Program	IAB and Academic Partners	14, 116, 119
Promoting and participating in dissemination activities	IAB and Industry Partners	88, 119
Mentoring and supporting students through an industry expert panel	IAB Members	84, 127
Collaborating with academia and industry in designing and delivering educational content	IAB Members	116, 119
Hosting real-life cybersecurity challenges and participating in collaborative projects	IAB Members	81, 119

Task/Activity	Responsible Party	Page Number
Participating in developing an EU-wide communications campaign	IAB and Consortium Partners	88, 127
Assisting in curriculum reviews based on changing industry needs	IAB Members	89, 126
Developing partnerships to expand the ecosystem of industry and education partners	IAB and Project Coordinator	88, 127

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