

D2.2: DIGITAL4Security Course Curriculum

Work Package 2, Task 2.2

Table of Contents

1. About the Digital4Security Project	3
2. The Digital4Security Consortium.....	3
3. Executive Summary	6
4. Introduction	8
4.1 Deliverable Objectives	8
4.2 Programme Objectives, Preliminaries and Inputs.....	9
4.3 Relationship to other WPs and Tasks.....	11
5. Overview of Curriculum Recommendations	13
5.1 ENISA Frameworks and Roles.....	13
5.2 Previous Projects and Recommendations on Curricula Design	15
5.2.1 Joint Task Force Guideline	16
5.2.2 Australian Computer Society Guideline	17
5.2.3 UK Cybersecurity Centre Guideline.....	17
5.2.4 USA National Centers of Academic Excellence	18
5.2.5 National Initiative for Cybersecurity Education (NICE).....	18
5.2.6 The Cyber Security Body of Knowledge (CyBOK).....	19
5.2.7 ENISA's Cybersecurity Skills Development in the EU	19
5.2.8 SPARTA Recommendations	20
5.2.9 REWIRE Online Trainings and Certification.....	21
5.2.10 Summary	21
5.3 Overview of existing study programmes in the EU	22
5.3.1 SPARTA existing study program analysis	22
5.3.2 ENISA CYBERHEAD database.....	22
5.3.3 REWIRE Existing Courses mapped to ENISA ECSF.....	24
5.3.4 Digital4Security WP6 Market Analysis.....	25
6. Methodology	25
6.1 Applied Concepts, Tools and Existing Content	25
6.1.1 ENISA ECSF Roles	25
6.1.2 Curricula Designer	28
6.2 Overview of Existing Courses Selection.....	32
6.2.1 Overview of Content provided by Partners.....	32

6.2.2 New Course Design.....	34
6.3 Main Steps of Curriculum Design.....	35
7. D4S Curricula.....	39
7.1 D4S two-year full-time master studies programme	39
7.2 Next Steps and Curriculum Maintenance.....	45
8. Conclusion	46
Appendices.....	49
Appendix A – Course Descriptions	49
Appendix B – Recommended Curriculum for CISO	109

1. About the Digital4Security Project

Digital4Security is a pioneering pan-European project developing a master's program to tackle the escalating challenges presented by cybersecurity threats and data privacy concerns across various industries. Backed by an international consortium consisting of 35 partners from 14 countries, this four-year project is funded by the European Union with nearly 20 million euros. The industry-driven program is set to convey extensive knowledge in cybersecurity management, regulatory compliance, and technical expertise to European SMEs and other companies.

In the scope of Work Package 2, the objective is to develop the curriculum for a two-year master's programme including micro-credentials and short courses. The program will offer training options tailored to students and professionals aspiring to pursue a career in cybersecurity management or to upskill to meet the everchanging market requirements.

2. The Digital4Security Consortium

The Digital4Security Consortium is an assembly of higher education institutions, industry partners, training providers, and cybersecurity clusters collaborating to craft, endorse, and implement an impactful cybersecurity management program. As a dynamic pan-European partnership, this initiative is composed of and executed by leading cybersecurity experts uniting innovators within the cybersecurity domain.

Partners	Acronym
UNIVERSITATEA POLITEHNICA DIN BUCURESTI	UNSTPB
SCHUMAN ASSOCIATES SCRL (SA)	
ATAYA & PARTNERS	ATAYA

POLITECNICO DI MILANO	POLIMI
POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	CMIP
CONTRADER SRL	CONTRADER
DIGITAL TECHNOLOGY SKILLS LIMITED	DTSL
INDEPENDENT PICTURES LIMITED	INDIEPICS
MATRIX INTERNET APPLICATIONS LIMITED	MATRIX
PROFIL KLETT D.O.O.	PROFIL KLETT
SERVICENOW IRELAND LIMITED	SERVICENOW
UNIVERSITA DEGLI STUDI DI BRESCIA	UNIBS
UNIVERSITY OF DIGITAL SCIENCE GGMBH	UDS
SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	SKILLNET
IT@CORK ASSOCIATION LIMITED	IT@CORK
ADECCO FORMAZIONE SRL	ADECCO TRAINING
UNIVERSITAT KOBLENZ	UNI KO
VYSOKE UCENI TECHNICKE V BRNE	BUT
MUNSTER TECHNOLOGICAL UNIVERSITY	MTU
EUROPEAN DIGITAL SME ALLIANCE	DIGITAL SME
DIGITALEUROPE AISBL*	DIGITALEUROPE
MYKOLO ROMERIO UNIVERSITETAS	MRU
SVEUCILISTE U RIJECI	UNIRI
NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	NASK
UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA	UNIR
NATIONAL COLLEGE OF IRELAND	NCI
TERAWE TECHNOLOGIES LIMITED	TERAWE
CY CERGY PARIS UNIVERSITE	CY GERGY PARIS

BANCO SANTANDER SA	BANCO SANTANDER
G & N SILENSEC LTD	SILENSEC
RED OPEN S.R.L.	RED OPEN S.R.L.
VYTAUTO DIDZIOJO UNIVERSITETAS	VMU



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101123430.

Document Control Information

Project	Digital4Security
Document Title	Digital4Security Course Curriculum
Work Package Number	WP2
Deliverable Number	D2.2
Lead Beneficiary	BUT
Project Coordinator:	National University of Science and Technology Politehnica of Bucharest (UNSTPB)
Dissemination Level	Public — fully open
Authors	Jan Hajny, Lisa Moravek, Sara Ricci, Petr Dzurenda, Pavel Loutocky, Andrej Kristofik, Vaclav Stupka, Frantisek Kasl, Jakub Vostoupal (BUT)

Reviewers	Reviewers (BUT) 1 st level review (NCI) 2 nd level review (UNSTPB) final review
Description	The aim of the DIGITAL4Security Course Curriculum report is to describe the Digital4Security curricula for a full-time and part-time master studies programme and to explain the methodology, research and pedagogical decisions shaping the curriculum development process
Status	Final
Delivery Date	27.04.2024
Due date	30.04.2024
Approval Date:	31.05.2024

Revision history

Version	Date	Modified by	Comments
1	11.04.2024	Jan Hajny	Initial Draft
2	18.04.2024	Jan Hajny	Following Review by NCI
3	30.04.2024	Ciprian Mihai Dobre (UNSTPB)	Initial public review
4	03.06.2024	Jan Hajny	Final Version

3. Executive Summary

The lack of qualified cybersecurity professionals is increasingly visible in the job offers on databases all over Europe. The Digital4Security project aims to increase the number of trained professionals and cybersecurity graduates for management positions by combining the expertise of various European faculties and businesses to offer a state-of-the-art master's programme in Cybersecurity Management.

The Digital4Security Course Curriculum report provides the theoretical background and methodology applied to compose and design a curriculum that incorporates today's and tomorrow's needs in cybersecurity and is flexible to appeal to both students and employees.

It describes the study programs objectives and positions the curriculum development within the projects work package landscape (Chapter 4) before presenting a comprehensive summary of the European Union Agency for Cybersecurity's (ENISA) European Cybersecurity Skills Framework (ECSF)¹ (Section 5.1). Moreover, it outlines recommendations on cybersecurity education from various international cybersecurity agencies (Section 5.2), such as the Australian Computer Society Guideline, NIST NICE, CyBOK and others. These guidelines are being compared and combined with conclusions derived from earlier projects such as SPARTA, a Horizon 2020 project focusing on recommendations for the creation of cybersecurity study programs and trainings, and REWIRE, an ERASMUS+ project dealing with cybersecurity online trainings and certification methodology development. Especially their comprehensive study of existing study programs and training opportunities was extended by the comparison of contemporary study programs carried out at the onset of the Digital4Security Project in Work Package 6 (Section 5.3).

Furthermore, this report describes the methodology applied to create the curriculum (Chapter 6). It describes the underlying concepts connecting ENISA ECSF framework of skills and knowledge to course content and the tools used, such as the Curricula Designer software. It also provides an overview of existing courses which represented the starting point to create a competitive program (Section 6.2).

Based on the mapping of existing courses, the expected skills and knowledge and recommended procedures, a core curriculum of mandatory and elective subjects was created (presented in Chapter 7). This curriculum supports the six ENISA ECSF profiles chosen by the consortium as a result of a thorough market needs analysis within the wider industry network, as well as preparing students for a variety of other ECSF roles in cybersecurity management.

¹ ENISA: European Cybersecurity Skills Framework (ECSF). URL: <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>

Moreover, this chapter draws conclusions from the deliverable D2.1, the Digital4Security Need's Analysis report² and earlier studies on cybersecurity and curricula development mentioned above. It also presents gaps that were identified in existing courses and the new course content created because of this analysis (Section 6.2.2 and Chapter 7). As the field of cybersecurity is rapidly evolving the importance of adaptation, and a reflection of emerging trends in the study programme is part of the curriculum maintenance, an essential task following the roll-out of the programme.

4. Introduction

4.1 Deliverable Objectives

This report outlines the methodology, underlying research and fundamental design of the curriculum intended for the Digital4Security master's programme which aims to contribute significantly to the overarching goals of the DIGITAL Europe Programme by facilitating the integration of a substantial number of graduates into high-demand positions aligned with the ENISA European Cybersecurity Skills Framework (ECSF). As the D4S project seeks to address occupational roles crucial for the sustained security and prosperity of European businesses, the primary objective involves the reskilling and upskilling of graduates, professionals, managers, and business leaders endowing them with the requisite expertise in cybersecurity management. It thus caters to a broad target audience and their various needs are to be considered when designing a flexible study program. Therefore, the intended curriculum structure encompasses both a two-year 120 ECTS full-time and a three-year part-time online master's programme consisting of compulsory and elective subjects alongside short courses and individual modules featuring micro-credentials to upskill employees. This report contains the description of programme learning objectives, course modules and the necessity of interdisciplinary courses and transversal modules

² Somers, Carmel: *Digital4Security Needs Analysis Report* (D2.1), 2024.

to address the needs of a broad target audience. In addition, it opens up questions to be addressed in the material development and roll-out phase.

The key aim of this initiative is to conceptualize and implement a European cybersecurity master's programme characterized by its high degree of innovation, effectiveness, and sustainability. This program is envisioned to generate a continuous stream of qualified cybersecurity management experts, thereby mitigating the expanding cybersecurity skills gap that poses a threat to the stability of various European industries and public sector institutions. The intended outcome is an enhancement of their cybersecurity infrastructure and the establishment of robust incident prevention and management procedures.

4.2 Programme Objectives, Preliminaries and Inputs

In preparation of the curriculum, partners in Work Package 2, Task 2.1 carried out a need's analysis³ which strongly influenced the creation of the master's programme. Not only did it take into account existing studies on master programmes in cybersecurity in the European Union and requirements by the industry, but it carried out its own survey of industry partners' wishes and their requirements for future employees. It also delved into an analysis and re-evaluation of existing descriptions of skills and knowledge required for certain ECSF profiles, narrowing down the six ENISA ECSF profiles this programme aims at.

Equally as important was the realization that the D4S master's programme is going to address students and employees who do not necessarily hold a bachelor's degree in IT and thus will need to accommodate a varied target audience.

Following tasks leader and project management discussions, the following strategic decisions were made:

³ Somers, Carmel: *Digital4Security Needs Analysis Report* (D2.1), 2024.

1. Primarily, the program will be designed as a 2-year master's programme taught online in English. The program will be governed by a single centralized body and requires a minimum 120 ECTS credits obtained in a minimum of 4 semesters.
2. Hands-on experience may be offered in cyber-ranges and on-site, depending on availability. The concrete offer will depend on the course owners and will be detailed in upcoming tasks focused on course content development.
3. Applicants are required to have a bachelor's degree in any field, but the expected knowledge and skills need to be precisely identified and communicated before program deployment.
4. The study program's learning objectives aim to prepare for managerial positions in cybersecurity and are derived from the definitions of skills and knowledge required for the following ENISA ECSF Role Profiles:
 - P1. Chief Information Security Officer (CISO)
 - P2. Cyber Legal, Policy & Compliance Officer
 - P3. Cybersecurity Risk Manager
 - P4. Cyber Threat Intelligence Specialist
 - P5. Cybersecurity Educator
 - P6. Cybersecurity Auditor
5. The customisation of the program will be done through elective subjects. Mandatory subjects will be taught as a foundation to all students regardless of the preferred profiles. Selections of voluntary subjects is up to the students, but a "recommended walkthrough" will be given to students as part of the curriculum description.

To ensure a close collaboration and communication with EU cybersecurity agencies, the work on D2.2 was significantly influenced by feedback and consultations with external stakeholders, in particular the ENISA ECSF Working Group and its Academic Pilot Subgroup. Namely the programme learning objectives, the methodology and initial drafts of the proposed curriculum were discussed and commented within the working groups.

The **Programme Learning Objectives** of the Digital4Security master's programme represent a starting point for the design of the curriculum and include:

- Equip students with a comprehensive understanding of cybersecurity principles, practices, and technologies relevant to modern enterprises.

- Equip students with the knowledge, skills, and mindset necessary for long-term success in cybersecurity leadership roles across diverse industries, government agencies, and institutional settings.
- Foster a culture of continuous learning and professional development to enable graduates to adapt to evolving threats, technologies, and regulatory environments throughout their careers.
- Develop expertise in legal and regulatory frameworks pertaining to cybersecurity, ensuring compliance and effective risk mitigation.
- Cultivate leadership skills necessary for effectively managing cybersecurity initiatives within organizations, including strategic planning and resource allocation.
- Foster advanced knowledge in cyber threat intelligence analysis, enabling proactive identification, assessment, and mitigation of cyber threats.
- Prepare professionals to educate others on cybersecurity best practices, raising awareness and promoting a culture of cybersecurity within organizations and communities.
- Train individuals to effectively respond to cybersecurity incidents, minimizing the impact and restoring normal operations swiftly.
- Foster interdisciplinary collaboration and communication skills essential for effective cybersecurity teamwork and leadership.
- Develop expertise in cybersecurity governance frameworks and practices to ensure effective oversight, auditing, accountability, and alignment with organizational objectives.
- Recognize and explore emerging trends, best practices, and industry standards in cybersecurity

4.3 Relationship to other WPs and Tasks

To understand the requirements for the curriculum as well as the learning outcomes the Digital4Security programme is aiming at, Work Package 2 has been working closely with the project management (WP1), and various other work packages. The intensive phase of curriculum development saw involvement of almost all partners within the consortium. At the same time, Work Package 6, which deals with the sustainability of the Digital4Security project, was closely

collaborating. Their market analysis of existing study programs in cybersecurity in the EU alongside the comprehensive need's analysis in D2.1 have shaped the course development and pedagogical design of the programme. For example, the survey among industry networks carried out as part of D2.1 showed the need for both professional and transversal skills to deal with the everchanging challenges in the realm of cybersecurity.⁴

As a core objective of the project, the design of the curriculum supposed to be carried out by all 16 HEIs and various industry partners has seen an immense team effort and collaboration between academic and industry partners to collect information on existing courses within the consortium and an analysis of their suitability for the D4S curriculum. In this main phase of Work Package 2 the support from the project management and thus Work Package 1 was essential in orchestrating the cooperation of all partners. In designing the curriculum, there has been a close collaboration with partners leading Work Package 4 which is going to be concerned with the roll-out of the programme and thus highly relies on a timely and diligent delivery of the curriculum. During the collection and analysis of modules provided by academic partners, the accreditation and certification process (Task T2.3) was already considered, trickling into Work Package 3. Similarly, the course collection included information on materials and licences in preparation of the material and learning platform which WP3 is focusing on. Moreover, the curriculum presented in this report can be seen as a matrix providing the structure of the study programme, while content and delivery are still to be developed in WP3, Task 3.1: Creation of a suite of Ready-to-Use online Training Materials for the delivery of the online Masters. Based on the feedback from T3.1, the curricula will be further updated and adapted to upcoming needs in Task 2.6: Curriculum Maintenance.

Another task within WP2 is the employability strategy (T2.5) that is supposed to set up an alumni network with a close relationship to industry partners and has strong ties to both Work Package 6 and Work Package 5, as they rely on dissemination material and a strategy to target a potential audience. Other tasks within Work Package 2, such as the definition of industry certification

⁴ Somers, Carmel: *Digital4Security Needs Analysis Report (D2.1)*, 2024.

pathways and EU recognized accreditation or the design of a European mobility programme complemented and accompanied the curricula development process.

5. Overview of Curriculum Recommendations

5.1 ENISA Frameworks and Roles

The ENISA European Cybersecurity Skills Framework (ECSF)⁵ is a collaborative effort between ENISA and its ad-hoc working group aimed at establishing a shared understanding of roles, competencies, skills, and knowledge in cybersecurity. It aims to facilitate the recognition of cybersecurity skills and to assist in designing related training programs. As shown in Figure 1, the framework identifies twelve cybersecurity-related role profiles, each detailed with responsibilities, skills, synergies, and interdependencies.

⁵ ENISA: European Cybersecurity Skills Framework (ECSF). URL: <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>



Figure 1. European Cybersecurity Skills Framework (ECSF)

The ECSF describes each profile through a table containing:

- *Alternative Title(s)*: other possible titles for the same profile,
- *Summary statement*: the purpose of the profile,
- *Mission*: the rationale of the profile,
- *Deliverable(s)*: the relevance with the perspective from a non-Cybersecurity/Information and Communication Technologies (ICT) point of view,
- *Main task(s)*: the tasks performed by the profile,
- *Key skill(s)*: list of abilities for the profile,
- *Key knowledge*: list of essential knowledge for the profile,
- *e-Competences (from e-CF)*: list of e-Competence Framework (e-CF) competencies covered by the profile.

There are 84 key skills and 69 key knowledge fields across the framework. Specific attention is paid to the key skills and knowledge fields for each profile due to their relevance for curricula development. For instance, Figure 2 depicts the key skills and knowledge for the Cybersecurity Educator profile.

Key skill(s)	<ul style="list-style-type: none"> • 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 • 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
Key knowledge	<ul style="list-style-type: none"> • 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

Figure 2. Key skills and knowledge for the Cybersecurity Educator profile (ECSF)

The ENISA ECSF served as the main framework to link skills and knowledge to profiles.

5.2 Previous Projects and Recommendations on Curricula Design

The landscape of cybersecurity education is rapidly evolving to meet the growing demand for qualified professionals in the field. Various institutions, both governmental and non-governmental, have formulated guidelines and recommendations to shape the design of cybersecurity curricula.⁶

⁶ (ISC)². *Cybersecurity Workforce Study*. 2022. [https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study.pdf?rev=ae39d66a4616478792d38da57fb80564&hash=31B8381DC81AD70B9B6DA6FF84534B33](https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study.pdf?rev=ae39d66a4616478792d38da57fb80564&hash=31B8381DC81AD70B9B6DA6FF84534B33;);

These recommendations emphasize interdisciplinary approaches, practical skills development, and alignment with industry standard.⁷ In this section, we delve into the most relevant recommendations provided by renowned institutions and highlight previous projects that have contributed to shaping the cybersecurity education landscape.

In the following part, we analyse the most important activities identified on a global level that are often used as exemplary approaches. Furthermore, we provide an overview of selected activities that could serve as an inspiration for approaches in the design of education programs within our project and thus form a starting point for the creation of educational activities within our project.

5.2.1 Joint Task Force Guideline

The Joint Task Force on Cybersecurity Education (CSEC2017 JTF) released the first global curricular recommendations for cybersecurity education in 2017.⁸ These recommendations highlighted the often-overlooked interdisciplinary nature of cybersecurity education, prioritizing the integration of foundational computing principles with a diverse array of overarching concepts, inter alia the legal and ethical aspects and professional responsibilities. The CSEC2017 volume also outlines eight Knowledge Areas (KAs), combining theoretical concepts with practical skills and covering topics ranging from Data Security to Societal Security. By structuring curricula around these KAs, institutions can ensure comprehensive coverage of essential cybersecurity concepts.⁹

Stocktaking of Information Security Training Needs in Critical Sectors [online]. ENISA. 7. 12. 2017
<https://www.enisa.europa.eu/news/enisa-news/stocktaking-of-information-security-training-needs-in-critical-sectors>

⁷ Hajný et al. *Framework, Tools and Good Practices for Cybersecurity Curricula*. <https://hal.science/hal-03997196/>

⁸ ACM. *ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline*. <https://cybered.hosting.acm.org/wp/>

⁹ <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>

5.2.2 Australian Computer Society Guideline

The Australian Computer Society (ACS)¹⁰ offers Specialist Accreditation in Cyber Security, providing guidelines for courses that prepare graduates for expert roles in cybersecurity.¹¹ ACS accreditation criteria, based on the Skills Framework for the Information Age (SFIA)¹², emphasize the acquisition of professional skills such as independence, making strategic decisions or working with suppliers.¹³ Degree programs seeking accreditation must align with the Core Body Of Knowledge (CBoK) for ICT professionals, covering areas such as ICT Professional Knowledge, ICT Problem Solving, and Technology Resources.¹⁴ The ACS framework enables institutions to tailor curricula to specific cybersecurity professional roles while ensuring alignment with industry standards.

5.2.3 UK Cybersecurity Centre Guideline

The UK National Cybersecurity Centre (NCSC)¹⁵ does not provide an explicit curricula framework, nevertheless, it combines the academic and practical cybersecurity knowledge into certified bachelor and master degrees, whose requirements may be interpreted as relevant guidelines. That is apparent primarily within the requirements of the Bachelor's degrees in computer science, distinguishing one of the three types of certification – foundational computer science topics, broad foundation in cybersecurity, and specialization in digital forensics.¹⁶ Each pathway delineates specific topics, credit requirements, and learning outcomes, enabling universities to design curricula that cater to diverse student interests and career goals.¹⁷ By focusing on core

¹⁰ <https://www.acs.org.au/>

¹¹ <https://www.acs.org.au/content/dam/acs/acs-accreditation/ACS%20Information%20Sheet%20-%20Cyber%20Security%20Specialist%20Accreditation%20V1.0.pdf>

¹² <https://sfia-online.org/en/about-sfia/browsing-sfia>

¹³ Hajný et al. *Framework, Tools and Good Practices for Cybersecurity Curricula*. <https://hal.science/hal-03997196/>

¹⁴ <https://www.acs.org.au/content/dam/acs/acs-accreditation/CBoK%20V3.2.pdf>

¹⁵ <https://www.ncsc.gov.uk/>

¹⁶ ACEs-CSE recognition and degree certification [online]. National Cyber Security Centre. 2024 [accessed 7. 3. 2024]. <https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0>

¹⁷ ACEs-CSE recognition and degree certification [online]. National Cyber Security Centre. 2024 [accessed 7. 3. 2024]. <https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0>

cybersecurity competencies alongside foundational computer science knowledge, NCSC-certified programs equip graduates with the skills necessary to address cybersecurity challenges in various domains.¹⁸

5.2.4 USA National Centers of Academic Excellence

The National Security Agency (NSA) and Department of Homeland Security (DHS) focus on cybersecurity education through the National Centers of Academic Excellence (CAE) program (aimed at cyber operations and cyber defence).¹⁹ CAE accreditation ensures that institutions adhere to rigorous academic standards and offer curricula aligned with CAE Knowledge Units (KUs).²⁰ By mapping programs to foundational, core, and optional KUs, institutions can ensure comprehensive coverage of essential cybersecurity topics while allowing flexibility to tailor curricula to specific program goals.²¹ Additionally, CAE programs emphasize practical, hands-on learning experiences to enhance students' skills development and readiness for cybersecurity careers.

5.2.5 National Initiative for Cybersecurity Education (NICE)

The National Initiative for Cybersecurity Education (NICE) provides a standardized framework, the NICE Framework, to identify the knowledge, skills, and tasks required for cybersecurity work roles.²² By leveraging the NICE Framework, institutions can identify particular industry needs based

¹⁸ Hajný et al. *Framework, Tools and Good Practices for Cybersecurity Curricula*.

¹⁹ National Centers of Academic Excellence [online]. *National Security Agency*. 2024 [accessed 7. 3. 2024]. <https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/>

²⁰ National Centers of Academic Excellence in Cyber Defense Education Program (CAE-CDE) *Criteria for Measurement Bachelor, Master, and Doctoral Level*. National Security Agency and the Department of Homeland Security, 2019. https://www.iad.gov/NIETP/documents/Requirements/CAE_CDE_criteria.pdf

²¹ Hajný et al. *Framework, Tools and Good Practices for Cybersecurity Curricula*.

²² Petersen, R. et al. *Workforce Framework for Cybersecurity (NICE Framework)*. National Institute of Standards and Technology, 2020. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

on the specific skills, knowledge and tasks and align curricula with those needs accordingly.²³ By doing so, they can ensure that graduates possess the requisite competencies for cybersecurity roles.

5.2.6 The Cyber Security Body of Knowledge (CyBOK)

The CyBOK project aims to codify foundational knowledge in cybersecurity and provide a comprehensive guide for cybersecurity education.²⁴ By identifying 19 Knowledge Areas (KAs) organized into five categories, CyBOK offers a structured framework for designing cybersecurity curricula.²⁵ Institutions can use CyBOK as a reference to ensure that their programs cover essential cybersecurity concepts and provide students with a solid foundation in the field. Moreover, CyBOK facilitates comparisons across different curricular frameworks, enabling institutions to identify common areas of focus and variations in emphasis.²⁶

5.2.7 ENISA's Cybersecurity Skills Development in the EU

ENISA's recommendations highlight the importance of structured curricula, practical training components, high-quality teaching faculty, interdisciplinary focus, outreach activities, and collaboration with industry stakeholders. By incorporating these elements into cybersecurity education programs, institutions can enhance students' readiness for cybersecurity careers and address skill shortages in the field.²⁷ Furthermore, ENISA has created the Cybersecurity Higher

²³ Hajný et al. *Framework, Tools and Good Practices for Cybersecurity Curricula*.

²⁴ Hajný et al. *Framework, Tools and Good Practices for Cybersecurity Curricula*.; The Cyber Security Body of Knowledge [online]. CyBOK. 27. 4. 2023 [accessed 29. 4. 2023]. <https://www.cybok.org/>

²⁵ *The Cyber Security Body of Knowledge*, 2023.

²⁶ E.g., Hallett, J., Larson, R., Rashid, A. *Mirror, Mirror, On the Wall: What are we Teaching Them All? Characterising the Focus of Cybersecurity Curricular Frameworks*. USENIX Association, 2018. <https://www.usenix.org/conference/ase18/presentation/hallett>

²⁷ De Zan, T., Di Franco, F. *Cybersecurity Skills Development in the EU*. ENISA, 2019. <https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union>

Education Database, which serves as a valuable resource for individuals seeking to enhance their cybersecurity knowledge and skills.²⁸

5.2.8 SPARTA Recommendations

The SPARTA project aimed to provide practical tools and strategies to help higher education providers design good cybersecurity curricula. In SPARTA Deliverable D9.2 ²⁹, 89 study programs in cybersecurity existing worldwide were analysed, and with the collection of recommendations from renowned institutions within and outside the EU, a methodology to develop higher education study programs and professional training courses is highlighted.

This analysis highlights the lack of standardization across countries and universities, with interdisciplinary collaboration often necessary due to the multifaceted nature of cybersecurity. There is a notable lack of bachelor's programs focused on cybersecurity, indicating a need for early exposure to cybersecurity subjects in students' studies. Additionally, internationalization of curricula is essential to broaden accessibility and relevance.

Moreover, cyber ranges are identified as a promising technology to provide students with hands-on training opportunities in virtual environments. Recommendations for bachelor's and master's programs emphasize the importance of practical lectures, with some programs having over 75% of lectures with hands-on training. This emphasis on practical experience reflects the evolving needs of the cybersecurity field and aims to better prepare students for the job market.

²⁸ CYBERHEAD – Cybersecurity Higher Education Database [online]. *ENISA – CYBERHEAD Map*. 25. 4. 2023 [accessed 29. 4. 2023]. <https://www.enisa.europa.eu/topics/education/cyberhead>; Nurse, J. R. C. et al. Addressing Skills Shortage and Gap Through Higher Education [online]. *ENISA*. 2021 [accessed 3. 5. 2022]. <https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education>

²⁹ Jan Hajny. 2020. D9.2 Curricula descriptions. <https://www.sparta.eu/deliverables/>

5.2.9 REWIRE Online Trainings and Certification

To address the shortage of cybersecurity experts, the REWIRE project proposed a multi-criteria selection method to increase the availability, accessibility, and quality of cybersecurity courses and certifications³⁰. The methodology considers six criteria and provides a scoring system to rank occupational profiles and select the most relevant ones for course design. The REWIRE final score formula identifies Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Threat Intelligence Specialist, and Penetration Tester for course creation.

Subsequently, the project proceeded with the development of an online training for the aforementioned ENISA profiles. Cyber ranges and virtual learning environments are used as integrated tools in the training. What is more, certification schemes have been developed, and students receive a certificate after passing an examination.

5.2.10 Summary

According to the analysis above, it is evident that each of the activities is different, and the area of cybersecurity is not comprehensively covered. In our activities and the focus in the context of the development of pan-European cybersecurity education, it is necessary to focus in particular on the complexity and requirements for different types of professionals, thus we reflect the above mentioned and further draw methodologically on the ECSF framework, providing complex education to comprehensively satisfy the requirements and needs related to cybersecurity education for the necessary roles, defined in the ECSF framework.

³⁰ Briones Delgado A, Ricci S, Chatzopoulou A, Cegan J, Dzurenda P, Koutoudis I. Enhancing Cybersecurity Education in Europe: The REWIRE's Course Selection Methodology. In Proceedings of the 18th International Conference on Availability, Reliability and Security 2023 Aug 29 (pp. 1-7)

5.3 Overview of existing study programmes in the EU

5.3.1 SPARTA existing study program analysis

In SPARTA Deliverable D9.2³¹, a sample of 89 existing study programs in cybersecurity was analysed across 59 universities. Specifically, 19 bachelor's and 70 master's programs were considered, spread over 19 EU countries, of which 5 are non-EU countries. In order to compare the curricula, the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) framework was used and expanded to better fit the academic and European context. Notably, the ENISA ECSF framework was still not developed at the time of the deliverable generation.

The analysis reveals that 23% of the curricula are taught jointly and involve multiple faculties due to the interdisciplinary nature of cybersecurity. In particular, one bachelor's and four master's study programs are multi-university ones. Another significant finding is that 73% of the analysed master's programs are developed by Computer Science and Engineering departments.

It is emphasized that a greater number of students need to have the opportunity to study cybersecurity subjects from the first year of their studies, necessitating the development of more study programs.

5.3.2 ENISA CYBERHEAD database

The Cybersecurity Higher Education Database (CyberHEAD)³², supported by ENISA, stands as the most extensive validated repository of cybersecurity higher education programs across the EU and

³¹ Jan Hajny. 2020. D9.2 Curricula descriptions. <https://www.sparta.eu/deliverables/>

³² ENISA, "Cybersecurity Higher Education Database," 2024. Online. Available: <https://www.enisa.europa.eu/cyberhead>.

European Free Trade Association (EFTA) nations. The database is presented on the official ENISA webpage as a dynamic application, i.e., a map with higher education institutions, providing cybersecurity related degree programs. Its primary purpose is to connect promising students with universities offering cybersecurity courses. Currently, it contains 145 curricula, specifically 30 bachelor's, 108 master's, and seven PhD programs.

In addition to the program type indicator, there is the possibility to search programs according to delivery type (online, classroom or blended), costs of the programs (free of charges or charges apply), language of the program and country. Notably, only 19 over the 145 curricula are delivered online, i.e., 17 master's and two bachelor's programs. Each curriculum is mapped to the ECSF profiles, facilitating students in making informed learning choices and understanding potential career paths.

Additionally, the database provides information on the number of ECTS credits and five thematical components covered by each program. These areas include Security Computing/Engineering, Law, Ethics, Policy, Cybercrime, Organizational Risk Management, Business Compliance, Internship, and Other.

It is important to note that CyberHEAD is a crowd-sourced database, meaning institutions have to apply themselves to be listed in it. The database is updated continuously, and institutions must fill out a standard application form when applying. This form contains information later presented in the program description. Before confirming the program and including it in the database, it is verified by ENISA. For degree programs to be eligible for inclusion in CyberHEAD, there are two core criteria. First, the degree must be recognized by a national authority of an EU or EFTA member state. Another requirement is related to cybersecurity-specific topics. For a bachelor's degree, at least 25% of the taught modules must be in cybersecurity topics, while this percentage is at least 40% for a master's degree. For a postgraduate specialization program outside the Bologna-degree structure, in addition to the requirement of at least 40% of the taught modules being in cybersecurity topics, another requirement of a minimum of 30 ECTS is applied.

5.3.3 REWIRE Existing Courses mapped to ENISA ECSF

The REWIRE R3.4.1³³ deliverable focuses on mapping existing cybersecurity training courses, university curricula, and certification schemes to the ENISA ECSF framework. This report examines the courses gathered from the four pilots (i.e., SPARTA, CONCORDIA, ECHO, CyberSec4Europe), enriches them, and aligns them with the framework.

The mapping methodology involves clustering ENISA key skills and knowledge described in the profiles into 31 REWIRE skill groups, as the key skills and knowledge are mainly uniquely phrased. Therefore, it does not allow for depicting the relationships among the profiles through the connections of the same skills and knowledge. Among the results from all four pilots, only the databases from SPARTA and CONCORDIA could be utilized for this task. CONCORDIA uniquely provides a map of professional training, while SPARTA maps university curricula using SPARTA topics aligned with the NIST NICE framework. Consequently, curricula can be seamlessly mapped to the ECSF framework. Unfortunately, none of the pilots dealt with certification scheme databases. Curricula, trainings, and certifications were analysed through the grouping and then linked to the 12 job profiles. A total of 85 curricula, 39 training programs, and 15 certification schemes were collected and categorized depending on which REWIRE groups and ENISA skills and knowledge they cover.

The analysis reveals the most frequent REWIRE skills groups in the collected curricula, training programs, and certifications. As a result, the most covered ENISA profiles are identified, such as the Cyber Legal, Policy and Compliance Officer, Cybersecurity Architect, and Cybersecurity Implementer, respectively.

³³ Petr Dzurenda and Sara Ricci. 2023. R3.4.1 Mapping the framework to existing courses and schemes. Online. <https://rewireproject.eu/deliverables/>

Moreover, the similarity of the output among curricula, training programs, and certifications was analysed. For instance, one of the most recognized profiles is the Cybersecurity Architect.

5.3.4 Digital4Security WP6 Market Analysis

D4S Work Package 6 focuses on developing a long-term sustainability strategy for the master's programme currently under development. To achieve this, an analysis of existing curricula with similar orientations has been conducted. 55 master programs of 90-120 ECTS and one specialization of four months were evaluated. Out of these 34 were full-time one campus, 14 online and 7 blended study programs combining on-site and online learning. In another survey carried out by consortium partners from the respective countries only 17 of the 91 cybersecurity master study programs were particularly aimed at Cybersecurity Management, while the rest was rather technical. These findings supported the wish to create a master's programme in cybersecurity with an operational and management focus.³⁴

6. Methodology

6.1 Applied Concepts, Tools and Existing Content

6.1.1 ENISA ECSF Roles

The ENISA ECSF³⁵ is embedded in our methodology as the core concept for linking role profiles with respective skills and knowledge that are required of our graduates by future employers. As

³⁴ Digital4Security Work Package 6 Market Research Results presented internally 26.02.2024

³⁵ European Cybersecurity Skills Framework Role Profiles
<https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>

planned in the project proposal, the Digital4Security's master's programme is going to focus on those ECSF profiles that are management oriented. In particular, seven profiles were selected in the project proposal: The Chief Information Security Officer (CISO), the Cyber Legal, Policy & Compliance Officer, the Cybersecurity Risk Manager, the Cyber Threat Intelligence Specialist, the Cybersecurity Educator, the Cybersecurity Auditor, and the Digital Forensics Investigator.

The Chief Information Security Officer (CISO) is responsible for managing an organization's cybersecurity strategy and implementation to ensure the security and protection of digital systems, services, and assets. Following the ECSF description, the CISO's more recurrent skills are on leadership and strategy development and risk management and compliance. Therefore, this profile must have the ability to develop and lead the execution of a cybersecurity strategy aligned with organizational objectives. Moreover, the CISO should be able to identify and solve cybersecurity-related issues and anticipate cybersecurity threats and challenges.

The Cyber Legal, Policy & Compliance Officer is responsible for managing compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organization's strategy and legal requirements. Following the ECSF description, the Cyber Legal Policy and Compliance officer's more recurrent skills are on legal and regulatory compliance and policy development and communication. In particular, this officer must have a comprehensive understanding of data privacy and data protection standards, laws, and regulations. Furthermore, they should be able to lead the development of cybersecurity and privacy policies that align with business needs and legal requirements.

The Cybersecurity Risk Manager is responsible for managing an organization's cybersecurity-related risks in alignment with its strategy. This profile must be able to establish a risk management strategy for the organization, select mitigation actions and controls, and to ensure that risks remain at an acceptable level. Additionally, the risk manager should possess strong communication skills to enable business asset owners, executives, and other stakeholders to make informed decisions regarding risk management and mitigation.

The Cyber Threat Intelligence Specialist is responsible for collecting, processing, analysing data, and producing actionable intelligence reports and disseminates them to target stakeholders. They manage the cyber threat intelligence life cycle. Besides, communication and collaboration skills are essential for the specialist to coordinate with internal and external stakeholders.

The Cybersecurity Educator is responsible for improving cybersecurity knowledge, skills, and competencies of learners. They must possess the ability to identify needs in cybersecurity awareness, training, and education and design and deliver learning programs to cover those needs. Communication skills are also essential for this profile.

The Cybersecurity Auditor is responsible for reviewing an organization's cybersecurity state, controlling processes, hardware and software while remaining integrity. They provide comprehensive reviews and audits of online security systems in accordance with regulations and frameworks. They identify security loop holes, protect critical data and increase the effectiveness of a company's security environment.

The Digital Forensics Investigator is responsible for ensuring that cybercriminal investigations reveal all digital evidence necessary to prove malicious activity. Following the ECSF description, the Digital Forensics Investigator more recurrent skill is ethical and independent investigation. This profile should be able to collect information while preserving its integrity and maintain objectivity throughout the investigation process.

In Deliverable 2.1, the “DIGITAL4Security Needs Analysis Report”³⁶, an analysis aimed to identify knowledge and skills requirements for the aforementioned seven cybersecurity roles was carried out. Notably, the Digital Forensics Investigator role stands out for its technical and ethical focus on collecting and analysing digital evidence. In contrast, Cyber Legal Policy & Compliance Officer

³⁶ Carmel Somers, D2.1 DIGITAL4Security Needs Analysis Report. February 2024

and Cybersecurity Auditor, prioritize compliance and legal aspects, The Cyber Threat Intelligence Specialist and Cybersecurity Educator roles are more oriented towards analysis, training, and education in cybersecurity, while the Cybersecurity Risk Manager is focused on risk management and mitigation. Given this distinction and after careful analysis, the consortium decided to exclude the Digital Forensics Investigator profile from the master's program curriculum. This choice is due to the specialized nature of digital forensics skills, which does not align with the broader objectives of the program. In fact, our program is going to focus on leadership and strategic aspects of cybersecurity to provide comprehensive education relevant to various cybersecurity roles.

6.1.2 Curricula Designer

The Curricula Designer³⁷ is a web application that allows users to create new or upload existing higher education study programs and analyse their content according to requirements of work roles on the job market. Naturally, this software was selected as the perfect tool to draft a first version of a curriculum and its analysis with respect to ENISA ECSF requirements.

The tool is divided into three sections as shown in Figure 4. The left section, marked as “1”, allows users to define new courses, the middle section, marked as “2”, allows the composition of a study program from defined courses, and the right section, marked as “3”, provides the statistical data and compliance of the designed program with certain requirements.

In Section 1, users can add a new course using the button “Add Course”.

³⁷ SPARTA Cybersecurity Curricula Designer <https://www.sparta.eu/curricula-designer/>

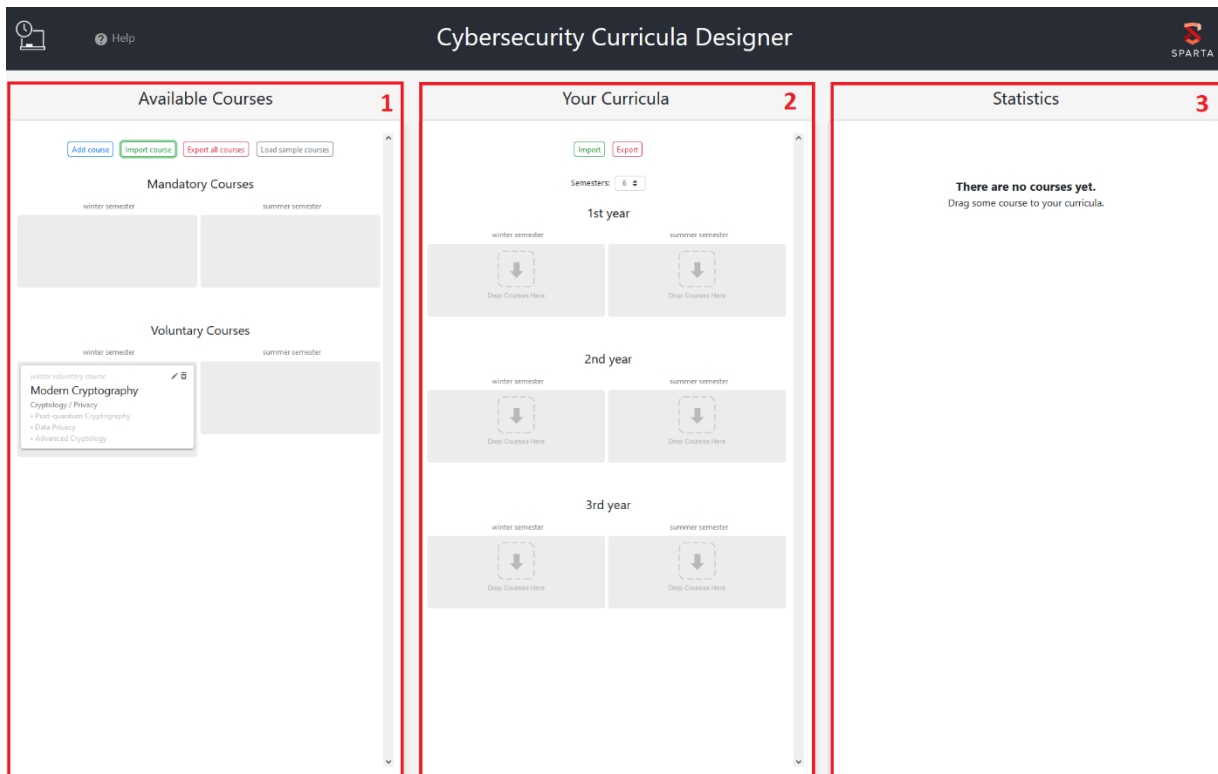
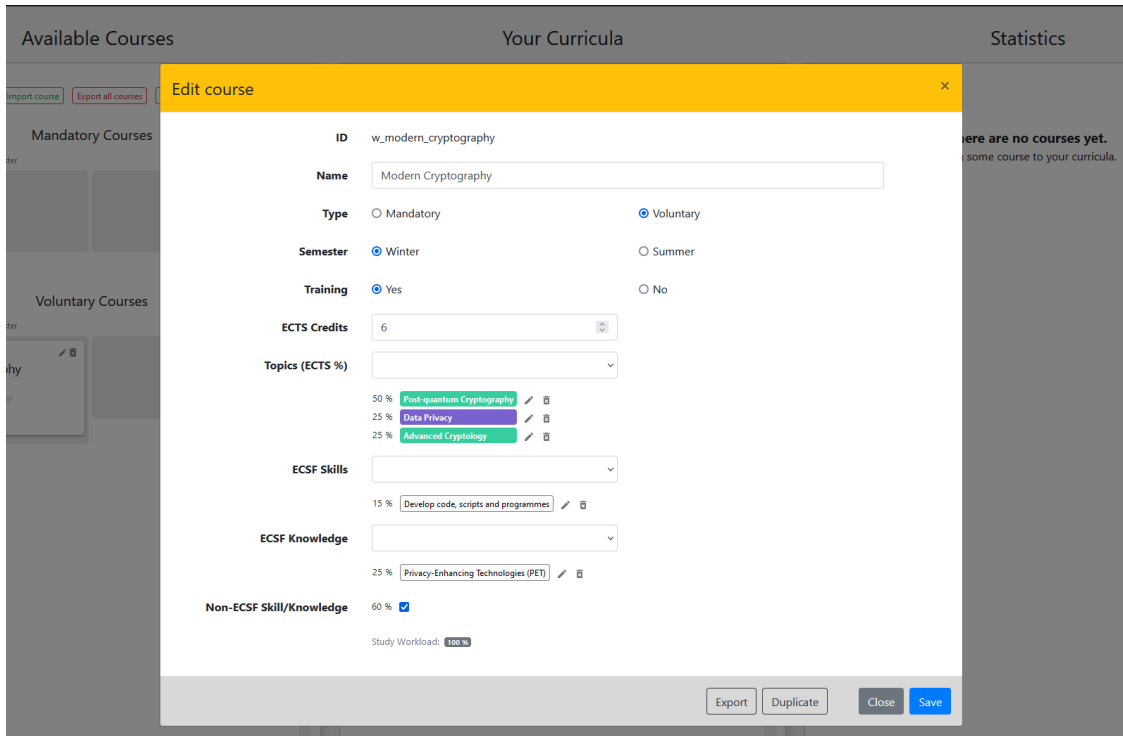


Figure 4. Designer GUI

Figure 5 shows an example for the addition of the course “Modern Cryptography”. Information required to be filled in here is the course name, type, semester, whether it includes practical training, the number of ECTS credits and the selection of topics, ECSF skills and knowledge that the course covers. Further, it is possible to edit and delete a saved course. Finally, the button “Export all courses” and “Import course” permits the downloading and uploading of a .json file of the created courses for future use.

Courses can be added to the study program by dragging the course box into the designated section representing a specific semester (such as summer, winter, year 1, 2). The application automatically verifies the semester and prevents insertion into an incorrect semester.



Available Courses **Your Curricula** **Statistics**

Edit course [X]

ID: w_modern_cryptography

Name: Modern Cryptography

Type: ☐ Mandatory ☒ Voluntary

Semester: ☒ Winter ☐ Summer

Training: ☒ Yes ☐ No

ECTS Credits: 6

Topics (ECTS %):

- 50 % Post-quantum Cryptography
- 25 % Data Privacy
- 25 % Advanced Cryptology

ECSF Skills:

- 15 % Develop code, scripts and programmes

ECSF Knowledge:

- 25 % Privacy-Enhancing Technologies (PET)

Non-ECSF Skill/Knowledge: 60 % ☒

Study Workload: 100%

Export Duplicate Close Save

Figure 5. Add course Tab.

In Section 3, statistical information about the study program is displayed. This information includes the distribution of credits in semesters, the distribution of ECTS credits to SPARTA areas, supported NIST NICE competencies and work roles. Most importantly, this section shows the covered ENISA ECSF profiles with missing skills and knowledge as shown in Figure 6.

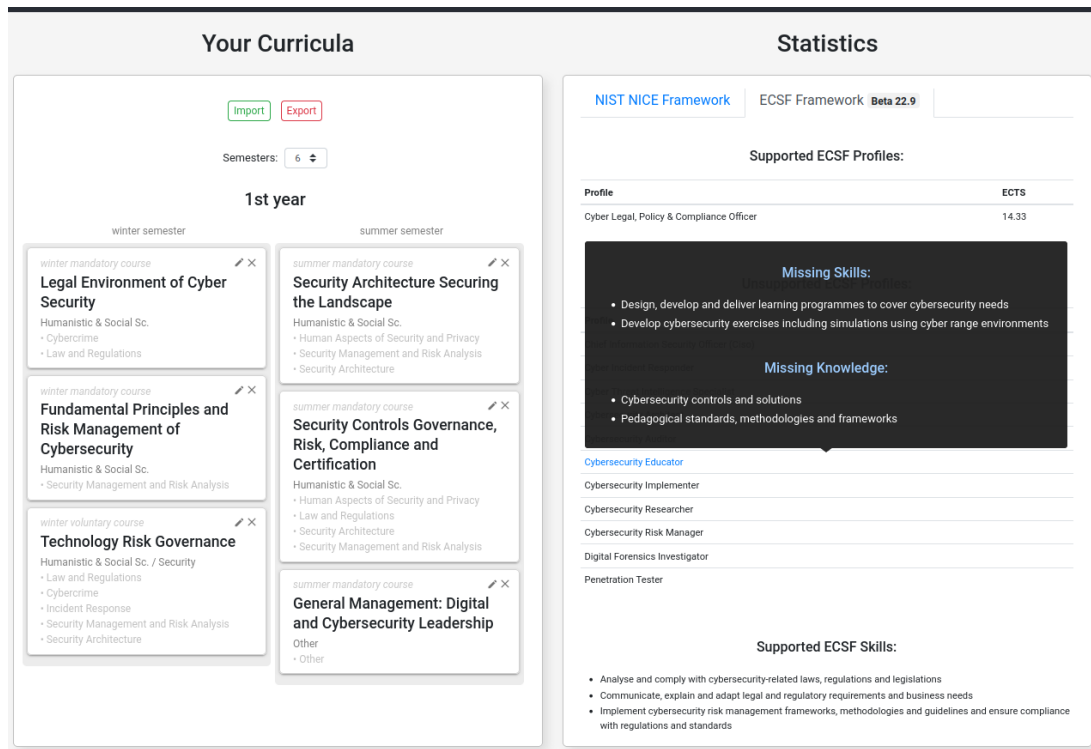


Figure 6. Statistics section showing missing skills and knowledge.

During the work on Deliverable 2.2, the Curricula Designer tool was significantly extended. In particular, the features for course and curricula export and import were added. Furthermore, a detailed analysis of knowledge and skills with respect to selected role profiles was added. In its current form, the Curricula Designer can be used not only for drafting the curriculum, but also for identification of knowledge and skills that are missing and for balancing the workload among suggested role profiles. The recommended curricula for selected role profiles are presented not only in this report (Appendix B), but also in the form of .json files importable to the Curricula Designer.

6.2 Overview of Existing Courses Selection

6.2.1 Overview of Content provided by Partners

The foundation of the D4S Cybersecurity Master's Programme consists of courses already being taught by partners in the consortium. These include universities and other higher education institutions as well as training providers from the industry. Their offer covers the four main areas of cybersecurity skills and knowledge described in the technical description of the Project Proposal³⁸ and confirmed as part of the findings of D2.1 that are technical, regulatory, incident response and management. With regards to technical skills only foundation courses were considered as mandatory courses while more advanced courses are recommended electives for more technical roles such as Cyber Threat Intelligence Specialists.

The need's analysis found that among the skills and knowledge most needed for the chosen cybersecurity roles, technical skills addressing AI are especially favoured by employers. Other technical skills required for cybersecurity management roles include technology fluency, enterprise architecture and infrastructure design, network fundamentals and system administration knowledge³⁹. These findings are reflected in the choice of mandatory courses presented in chapter 7.

Figure 7 shows professional and transversal skills identified by the survey carried out in T2.1. These formed the basis for the selection of suitable courses from within the existing subjects offered by partners.

³⁸ Digital4Security Proposal, technical description (Part B), p.4.

³⁹ Somers, Carmel: *Digital4Security Needs Analysis Report* (D2.1), 2024, p. 31.

Professional Skills	Score	Transversal Skills	Score
AI	64	Communications	39
Law/Legal, Policy, Ethics	54	Leadership/Management Skills	11
Risk	46	Project Management	5
Threat Management/Analysis	43	Stakeholder Management	2
Business / Business Process	42	Analytical Skills	2
Incident Management	22	Change Management	2
Intelligence Analysis	20	Adaptability	2
Cloud	13	Problem Solving	2
Compliance	10	Decision Making	1
Forensics	9	Critical Thinking	1
Governance	7	Report Writing	1
Privacy / Data Privacy	6	Mentoring/Tutoring	1
Testing	6	Methodical Working	1
Audit	4		
Blockchain	3		
Automation	3		
Geopolitical	2		

Figure 7: Professional and transversal skills identified by the survey

With regards to diversity in methodology, the presented courses offer a variety of blended and online learning, cyber ranges, labs and cybersecurity datasets available for trainings. During the selection of suitable courses, additional material such as more than 1000 hrs of training scenarios provided by Adecco, security Challenges from ServiceNow and cyber ranges from Silensec were collected to be used during the material creation in Work Package 3, task 3.2 or for additional trainings. This input from industry partners complements the academic subjects to give a holistic and hands-on experience.

Since teamwork across different disciplines has long been reality in IT companies, “preparing cybersecurity students to be job-ready requires educators to design learning experiences that develop teamwork skills across the course of study”⁴⁰. As the selection of courses was reviewed

⁴⁰ Hall, J., Rao, A.: „Enabling Teamwork in Cybersecurity Courses“, in: Sikos, L.F., Haskell-Dowland, P.: *Cybersecurity Teaching in Higher Education*. Springer 2023, p. 79

and reconsidered by various partners a few gaps were identified that formed the basis for considerations around new course content.

6.2.2 New Course Design

The comparison of required topics, skills and knowledge to cover all six ENISA profiles with the actual courses on offer resulted in the discovery of gaps concerning both topics and skills or knowledge. Simultaneously, the need's analysis revealed “hot topics” that employers wished their employees to be familiar with and an array of mainly transversal skills that had so far not been in the focus of programs offered by more technical universities.

This discovery was congruent with the evaluation the consortium members made when drafting curricula during a workshop in Dublin in March 2024. Against the backdrop of a theoretical analysis the voices of industry partners echoed the same concern that inspired the suggestion of the following subjects:

- A course on the **Foundations of Pedagogy and Didactics for Cybersecurity Educators**. This subject combines the theory of learning with hand-on seminars on course planning and delivery based on didactic principles of adult learning with a focus on planning, methodology, material design, and communication. Instead of only focusing on mitigation human risks students will learn to actively enhance defences by fostering a culture of more security-aware people.
- A course dealing with **Emerging Technologies** and their benefits and risks for cybersecurity such as AI, blockchain, (post-)quantum, IoT, autonomous systems, social media, chain of custody, business continuity etc.
- A course accompanying **practice in companies**,
- A course on **Cybersecurity Auditing**
- Writing a master's **thesis**

While these new courses are being suggested, they have not been fully designed at the time of the submission of this report. For once, third parties, such as Microsoft might offer a solution suitable for the D4S master's programme. Another more likely possibility would be, that industry partners would take on this task. Either way 15-20 ECTS within the program are reserved for new content,

consisting of short courses that can form voluntary courses in the full-time program⁴¹. As new trends and technologies emerge, it is also advisable to observe the developments and create short courses on relevant topics at a later point closer to the program roll-out or as part of the Curriculum Maintenance task 2.6. Similarly, partners in Task 2.5 are developing an industry network and creating letters of intent that might increase collaboration with the industry.

It is exactly this collaboration and interaction between academia and the industry that the last “new” course is aiming at, by offering full time students an industry internship on-site at a company. This should ensure hands-on experience and might be offered as part of the D4S mobility program. When completing the internship within this course, students will be provided assistance in navigating their placement, guidance on enhancing their learning from the acquired experiences, and instruction on how to use these experiences during their own job search. It contains the theoretical preparation of an industry internship at a company while offering input for analytical reflexion during and after the work experience.

Another additional mandatory course is the research project for the master thesis. Here students use the online learning platform to contact a supervisor and suggest a research topic for their master’s thesis that reflects the specialisation they have chosen.

6.3 Main Steps of Curriculum Design

Designing cybersecurity curricula is a rather new discipline. There were very few programs focused on cybersecurity only a decade ago and these were usually only slight modifications of existing programs, such as Computer Science or Informatics. However, the dynamic evolution of digital technologies and the rising number and complexity of cyberattacks created an urgent need for the deployment of new programs. So far, the creation of novel programs focused on cybersecurity has

⁴¹ At the time of writing this report, Terawe and Skillnet Ireland have been considered for this task.

been rather uncoordinated and unstructured, usually heavily depending on existing programs, courses, and capacities of universities and training providers. Until only recently, there were no good practices for creating cybersecurity study programs, no common framework, or even a common vocabulary to use. As a result, various programs of different names (e.g. Cybersecurity, Computer Security, Information Security, Network Security etc.) and focus (technical, management, legal) were created, without providing much of mutual interoperability and possibility of study exchanges.

The unstructured and rather “wild” design of study programs has led to several issues, such as:

- difficult student exchange due to a disharmonized content,
- unclear focus of study programs and skill gaps between provided education and needs of the job market,
- incomplete coverage of all domains relevant for cybersecurity, i.e., missing legal/social components in technical programs and vice versa,
- absence of coverage of recent and upcoming topics and key technologies, such as quantum, blockchain, AI.

In Digital4Security, we are aware of these issues and attempt to avoid them by using a structured and consistent approach to create the curriculum. We tap into the recently published ENISA ECSF framework as the core method for the categorization of work roles and identification of knowledge and skills that are required by specific roles. In using the ECSF framework, our methodology is repeatable, common for all EU countries and reflecting all disciplines and topics relevant to cybersecurity.

The main steps for the D4S curriculum design were already identified at the D4S kick-off consortium meeting in Bucharest in 2023. Here, the ENISA ECSF framework and the Curricula Designer tool were introduced to all partners and the basic methodology was outlined. Since then, the curriculum has been developed in Task 2.2 following these steps:

1. **Selection of ECSF Role Profiles:** The D4S study program is by design focused on Cybersecurity Management and therefore differs from existing technical programs. In the

project proposal, seven ECSF Role Profiles reflecting this focus were selected. In Task 2.1, which contained consultations with employers and industry, this focus was narrowed down to the final six role profiles:

- P1. Chief Information Security Officer (CISO)
- P2. Cyber Legal Policy & Compliance Officer
- P3. Cybersecurity Risk Manager
- P4. Cyber Threat Intelligence Specialist
- P5. Cybersecurity Educator
- P6. Cybersecurity Auditor

More information on this step can be found in deliverable D2.1.

2. **Analysis of Market Needs:** Having identified the main role profiles, the D4S consortium collected feedback from academia, industry, and public sector on expectations of program graduates. Skills and knowledge that are required for selected profiles were identified and the description already present in the ECSF framework was expanded and instantiated. Furthermore, the prioritization of knowledge and skills was done in Task 2.1. More information on this step can be found in deliverable D2.1.
3. **Analysis of Existing Programs:** As part of the D4S curriculum design, the analysis of existing programs was completed to avoid duplicates and fill in gaps in the offer of study programs. In this activity, we partially relied on the work done in previous projects, such as SPARTA, REWIRE, CONCORDIA, and official public sources, such as the ENISA CyberHEAD database. This analysis confirmed the original aim to focus on management-, governance- and law-related content. More information about this activity is provided in Section 5.2.
4. **Collection of Existing Courses within the Consortium:** To create a starting point for a discussion, basic information on courses related to cybersecurity currently being taught by universities and training providers from the consortium were collected. These included descriptions of courses, ECTS, language, owners, and types of completion. From around 200 courses initially collected, 103 courses taught in English were further evaluated by experts among the consortium who first identified their own area of expertise (governance, management, technical or incident response) and then evaluated each course regarding its

suitability for a cybersecurity management study program. More information can be found in section 6.3.

5. **Selection of Courses for the Curriculum:** All courses were evaluated by two experts in the given domain and courses with a minimum score of 3 out of 5 passed on for further evaluation. Based on the evaluation of domain experts, availability in English and licensing, the first set of courses for the D4S program was proposed.
6. **Design of Curriculum Draft:** Partners providing selected courses (called “course owners”) were asked to import their courses to the Curricula Designer tool and to identify skills and knowledge which their courses provide. Using the Curricula Designer, the first draft of the curriculum was created in such a way that all selected ESCF profiles are supported, i.e. all knowledge and skills required by ECSF are provided by selected courses within the limits given by the ECTS system.
7. **Identification of Missing Content:** Even though the existing courses covered most of the required knowledge and skills, there were some components still missing in the first draft of the curriculum. Therefore, new courses on pedagogy and didactics, as well as courses on emerging technologies, were added to the curriculum.
8. **Finalization of Curriculum, Creation of Derivates:** The first draft of the D4S curriculum was presented at the consortium meeting in Dublin in March 2024. A whole-day workshop was devoted to the finalization of the curricula, with participation of all members of the consortium, including industry representatives. The main part of the workshop consisted of a group activity, where participants were divided into working groups according to the Role Profile they prefer. The objective of each group was to update the provided curricula draft according to their needs and expectations. Any course could have been modified, removed, or added. As a result of this activity, we received six new curricula, each prepared for a particular Role Profile. Participants also identified gaps and made suggestions for new course content as described in section 6.2.2. Then, we compared these proposals, merged courses that were shared by at least three Role Profiles into the set of mandatory courses and left remaining courses as electives. Recommendations on the selection of voluntary courses based on their relevance to particular Role Profiles were drafted. As a result, we obtained a single curriculum with two sets of mandatory courses and voluntary courses, from which students can choose those reflecting their targeted role profile(s). The resulting

2-year master's programme curriculum serves as a starting point to create derivatives for the part-time program, micro credential courses and short courses. Due to a shared audience (which consist of students not willing to study classical presence study programs at universities, mostly working and appreciating the online form of study), we do not expect to have a significant difference in course content. Therefore, the part-time program is planned to be similar to the 2-year program but relaxed to 3-years. The micro credential programs are module components of the master, and short courses are represented by individual courses of the master's programme.

9. **Verification of the Curriculum Draft:** The pre-final draft of the curriculum was distributed to the whole D4S consortium with request for comments and modifications. Any course could be replaced, moved or added. A group of "testers" for each Role Profile was created, coordinated by an industry partner to check the alignment of the curriculum with needs of the job market. The final remarks have been reflected in the proposed draft, but the activity is ongoing and continues also in Task 2.6, Curricula Maintenance and Update. We expect that the curriculum presented in the next section will be further updated and improved, as new progress is made in the project, particularly regarding accreditation of the program and deployment, which are addressed in other WPs.

7. D4S Curricula

7.1 D4S two-year full-time master studies programme

The Digital4Security curriculum for the 2-year master's program is presented in Table 1. It consists of 73 ECTS credits in 11 mandatory courses, that are common for all six Role Profiles. These courses include five courses mainly focused on management, three technical courses, one legal course and two general courses, all of which are being taught in English⁴². The master's thesis is also mandatory. In addition, voluntary courses are provided, and recommendations are given with

⁴² At a later point the D4S programme might offer courses in other languages as well. For the first draft however, the curriculum and the study programme are monolingual as is the curriculum description in Appendix A and B of this report.

respect to their relevance to role profiles (column recommended profile). Students may choose any voluntary course in any year of study, though recommended courses and semesters are indicated in the table. Most of the courses already have an owner in the consortium, who is going to be responsible for course content delivery and maintenance. The concrete specifications of each course are provided in Appendix A, that provides information on all courses provided by partners of the consortium that were chosen as a starting point. While all partners were requested to supply courses, some courses might be harmonized as part of the rationalisation and modification of existing material in the next steps of curriculum development and content creation in line with the accreditation and certification process.

1. year of study, winter semester

abbr ev.	Title	ECTS	Type	Scope	Recommended Profile	Partner
ISS	Information System Security	6	compulsory	Technical	all	VDU
SFU	Security Fundamentals	8	compulsory	General	all	NCI
CBT	Cybersecurity Battleground: Threats, Vulnerabilities and Technologies	5	compulsory	Management	all	ATAYA
ISG	Information Security Governance	3	elective	Governance	P1, P2, P3,	CEFRIEL
ITG	IT Governance	6	elective	Governance	P3,	VDU
CCY	Communications & Cybersecurity	5	elective	Response	P1, P3,P4, P5	MTU
TCY	NEW - Training Cybersecurity - Foundations of Didactics I	5	elective	Response	P5,	TBD
SOC	Security Operations: Continuity and Crisis Management	5	elective	Response	P6	ATAYA
FAE	Forensics and eDiscovery	5	elective	Technical	P6	NCI
CAU	Cybersecurity Auditing	5	elective	Governance	P6	TBD

1. year of study, summer semester

TRG	Technology Risk Governance	5	compulsory	Management	all	POLIMI
ISL	Information Security Leadership (the CISO Fundamentals)	5	compulsory	Management	all	ATAYA
CAS	Cloud Architectures and Security	8	compulsory	Technical	all	NCI
SCG	Security Controls Governance, Risk, Compliance and Certification	5	elective	Governance	P1, P2, P3, P4, P5	ATAYA
LDA	Law and Data	5	elective	Governance	P2,	UNIBS
CCI	Cyberdefense and Cyberintelligence	5	elective	Management	P4,	UNSTPB
IGS	IT Governance, Security and Ethics	6	elective	Governance	P3	NCI
CAA	Cybercrime and Advanced Attack Tactics, Techniques and Technologies	3	elective	Technical	P4,	CEFRIEL
PAE	Principles of Advanced Enterprise Security	3	elective	Response	P4,	CEFRIEL
CET	NEW - Cybersecurity in Emerging Technologies	5	elective	Technical	P5, P6	TBD
SEC	Security Economics	4	elective	Management	P5	MRU
TCF	NEW - Training Cybersecurity - Foundations of Didactics II	5	elective	Management	P5	TBD
FPR	Fundamental Principles and Risk Management of Cybersecurity	6	elective	Management	P1	MRU

2. year of study, winter semester

ISM	Information Security Management	5	compulsory	Management	all	UNSTPB
CIS	The challenges for Information Security	3	compulsory	Technical	all	CEFRIEL

ACR	Applied Cryptography	5	elective	Technical	P2, P6	UNSTPB
SML	Security Management and Law	8	elective	Management	P1, P2, P4	MTU
FOC	Foundations of Cryptography	6	elective	Technical	P1, P2,	BUT
SAR	Security Architecture	8	elective	Technical	P1, P2, P3, P5	MTU
CCY	Communications & Cybersecurity	5	elective	Response	P3, P5	MTU
FPR	Fundamental Principles and Risk Management of Cybersecurity	6	elective	Response	P1,	MRU
OCS	Organizational Cyber Security Culture	6	elective	Management	P3	MRU
SCP	Security Contingency Planning	5	elective	Management	P4	MTU
ISG	Information Security Governance	3	elective	Governance	P5	CEFRIEL
OSY	Operating Systems	5	elective	Technical	P6	UNSTPB
CNS	Computer and Network Security	5	elective	Technical	P6	UNSTPB
AAD	Application, Accesses and Data in Security	3	elective	Technical	P6	CEFRIEL
NSP	Network Security and Penetration Testing	8	elective	Technical	P6	NCI

2. year of study, summer semester

THE	Thesis	15	compulsory	-	all	TBD
BRI	Business Resilience and Incident Management	5	compulsory	Management	all	NCI
CCR	Cybercrime and Cybersecurity	3	compulsory	Governance	all	BUT
SAS	Security Architecture - Securing the Landscape	5	compulsory	Technical	all	Ataya
CAA	Cybercrime and Advanced Attack Tactics, Techniques and Technologies	3	elective	Technical	P2	CEFRIEL
MIP	Management of IT Projects	6	elective	Management	P1	MRU
AIC	AI/ML in Cybersecurity	5	elective	Technical	P4	NCI
MA						
N	Malware Analysis	5	elective	Technical	P4	NCI
PRA	NEW - Practice in Company	10	elective		all	TBD

Table 1: D4S Master's Programme Curriculum

The overall structure of the curriculum is provided in Figure 8, together with the identification of micro-credential modules (Cybersecurity Management and Cybersecurity Technologies) that can be studied separately.

DIGITAL4Security

Masters Programme in Cybersecurity Management & Data Sovereignty

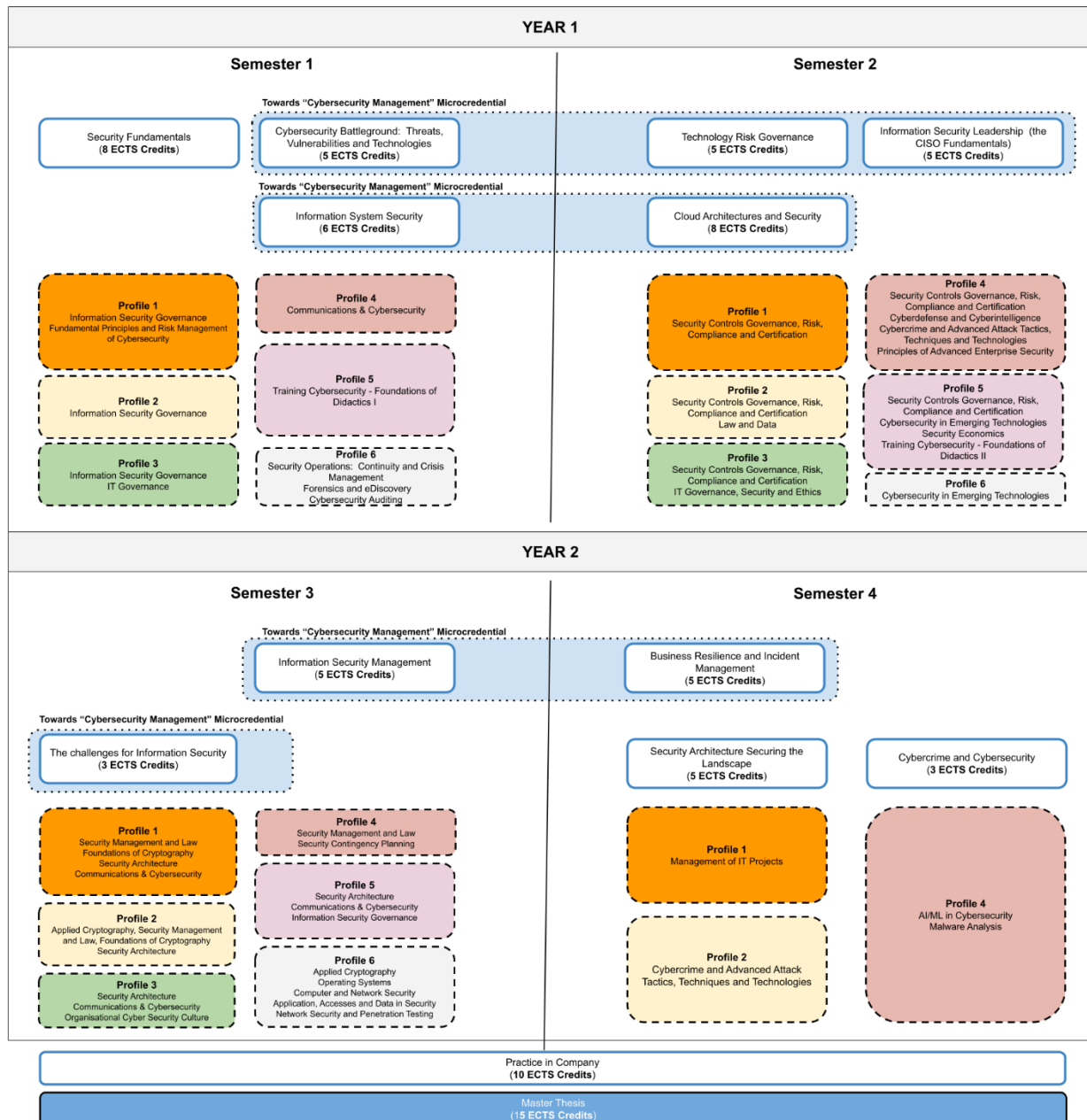


Figure 8: Overview of D4S Master's Programme in Cybersecurity Management & Data Sovereignty.

7.2 Next Steps and Curriculum Maintenance

The curriculum presented here for the two-year full-time master's study programme can be adapted for the three-year part-time programme and individual subjects lend themselves to be bundled in training modules for employees seeking to improve particular aspects of the interdisciplinary and everchanging cybersecurity landscape. We expect that the description and especially the content of courses will be further developed in WP3 to reflect different needs of full-time, part-time, micro credential and short-course programs.

The submission of this curriculum will set into motion the development of suitable and diverse content, material and an online learning platform to access it in Work Package 3, Tasks 3.1 and 3.2. With the specification of the course content that is planned to be delivered in T3.2, new requirements on prerequisites may arise, resulting in minor curricula updates. These will be incorporated in Task 2.6, Curricula Maintenance.

Outstanding tasks to complete and refine the curriculum include the development and design of the suggested new courses, inclusion of license information and completion of material repository set up by WP2 and used by WP3 as well as streamlining the ECTS amounts per course in a way that is in accordance with the accreditation body.

Furthermore, the new content suggested as a consequence of our findings is to be developed into engaging courses with innovative material covering the knowledge and skills' aspects needed to support all of the six ENISA ECSF role profiles chosen at the onset of this project. As the challenges facing companies, institutions and private people evolve, so will this curriculum, as content is to be continuously updated or replaced. This might in the future include modules delivered in other languages, as so far, the offer is guaranteed only in English. Feedback from the Industry Advisory Board recently set up, as well as working groups from within the consortium who volunteered to review the curricula suggestions are going to form part of the maintenance of the curriculum defined in Task 2.6.

A preliminary meeting in Brussels in June 2024 already hinted at some modifications, as valuable feedback was incorporated. Partners from the industry wished for the duration of the part-time program to be shortened to 2.5 years and for some suggested modules to be modified as they were considered too technical for a cybersecurity management profile.

Another decision was to align and comprise the program learning outcomes and to standardize module learning outcomes.

In another step ECTS for individual courses are to be harmonized. The vast offer of electives will likely be reduced to about 15 modules, of 5 ECTS each. This allows for a more clear and manageable offer of electives of which students should choose five.

The design of the D4S curriculum is an ongoing process with partners' feedback being respected and new developments in the dynamic field of cybersecurity closely followed and incorporated in future roll-outs. Equally, students' and participants' feedback are going to be valuable in the development of the programme. Moreover, the accreditation process may necessitate further modifications to the curriculum. These will be reported in task 2.6 as well as WP3 deliverables.

8. Conclusion

This report describes the curriculum that forms the foundation of the Digital4Security master's programme and training options and thus Milestone 2 in the D4S project. It details the theoretical frameworks and considerations the curriculum development is based on and gives an overview of the learning objectives for various target audiences. In addition, it outlines the skills and knowledge needed to perform various roles in the cybersecurity realm and the preparation, course modules and transdisciplinary courses students and professionals are going to receive throughout our programme. The curriculum presented in this document, including the micro credential modules and individual courses, serves as a guideline that still needs to be perfected by adjusting the actual content of courses. Based on the exact content delivered by T3.2, further changes are expected to be made in the curricula maintenance phase (T2.6).

Work Package 2/Name	WP2 Needs Analysis and Programme Design
Deliverable Name	D2.2 Curriculum Design Report
Partners involvement	BUT
Submission Deadline (As per Annual Work Plan)	30-04-2024

Rate	1	2	3	4	5
Quality Parameter	very low/strongly disagree	low/disagree	moderate/neither nor	high/agree	very high/strongly agree
1. The work performed corresponds to the requirements and methodological standards of the project.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. The drafting and structuring of each deliverable include the	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

contribution of all relevant experts.					
3. Deliverables use clear and easily understandable language in the text and the design is professional and in line with the project brand identity, guidelines, and document template.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. The output is in line with the standards adopted by the European Commission.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insert text here...					
Name of the WP Leader	Jan Hajny - Brno University of Technology				
Submission Date	03/06/2024				

Appendices

Appendix A – Course Descriptions

	Course #1
Partner Name	Brno University of Technology
Contact Person	Jan Hajny
Contact Email	hajny@vut.cz
Course(s) Name	Foundations of Cryptography
ECTS Credits	6
Labs available	Yes
Completion	Credit + Written Exam
Description	Basic terminology in cryptology, cryptology categorization, algebraic structures used in cryptography. Generation, testing and use of prime numbers. Group arithmetic. Complexity theory fundamentals. Computationally hard problems used in cryptography – discrete logarithm, RSA problem, EC discrete logarithm. The overview of basic algorithms used in cryptography. Symmetric and asymmetric cryptosystems (DES, AES, RSA, DH, ECDH, SHA2, 3) and their

	practical use. Provable security concept – proofs, formal models, zero-knowledge, Sigma-protocols.
Learning Outcomes	"During the course, students will study the theoretical foundations (mainly the algebraic structures and their properties), the most common algorithms and concepts used in modern cryptography. Students will obtain theoretical foundations of cryptography and computer security. Based on these foundations, students will be able to analyze and design security solutions for information and communication technologies (ICT). Students will be able to explain basic principles of algebraic structures used in cryptography, basic cryptographic primitives (hashes, RNG, provably secure protocols), basic algorithms and describe the internals of symmetric and asymmetric algorithms. Students will be theoretically prepared for follow-up courses from data transfer and ICT security areas."
Course/Material License	Open Source

	Course #2
Partner Name	Brno University of Technology
Contact Person	Jan Hajny
Contact Email	hajny@vut.cz
Course(s) Name	Cybercrime and Cybersecurity
ECTS Credits	3
Labs available	No
Completion	Oral exam
Description	Concept and structure of substantive and procedural criminal law, structure of typical cybercrimes, theory and practice of procedural

	tools used in prosecution of cybercrime, concept and structure of cybersecurity law, theory and practice of legal obligations of regulated subjects, liability for cybersecurity incident, European and international legal regulatory instruments in cybercrime and cybersecurity including certification in cybersecurity.
Learning Outcomes	Upon the completion of the course, students should be able to understand the structure and system of criminal law institutes used in investigation and prosecution of cybercrime as well as to apply these institutes in regular corporate and public practice. Besides fundamental substantive and procedural institutes, the course will focus also on discovery and forensic analysis of digital evidence including issues related to protection of privacy, protection of personal data and specifics connected to handling of electronic document including electronic identification. Students should also be able to understand and apply basic preventive and regulative legal instruments in cybersecurity and to critically assess relations between national legal regulatory framework and international harmonization instruments. In addition, students should be able to practically use legal instruments related to regular practice of cybersecurity incident response teams including aspects related to their reporting.
Course/Material License	Open Source

	Course #3
--	------------------

Partner Name	Vytautas Magnus University
Contact Person	Vytautas Barzdaitis
Contact Email	vytautas.barzdaitis@vdu.lt
Course(s) Name	Information System Security
ECTS Credits	6
Labs available	Yes
Completion	Credit + Written Exam
Description	Cryptography terminology, encryption algorithms and factors enhancing the security of electronic systems; information system auditing; multifactor authorization; ethical hacking; vulnerability of wireless internet stations; malware, analysis of top ten OWASP critical violations; electronic signature; using hash functions. identification and authentication; cloud computing and software development issues in the context of information systems security.
Learning Outcomes	Upon completion of this course, students will be able to characterize common types of cyber-attacks against information systems, identify information system security risks, analyze real cases, assessing cyber-security capabilities. They will have knowledge of risk management, access control, authentication technologies, cryptography, digital signature technologies, public and private key infrastructure. Students will be able to recognize main types of malware, explain main security principles of cryptographic systems, understand and be able to use different hash types. They will be capable of examining the vulnerabilities in the OWASP top 10, and will be familiar with the use of ethical hacking for strengthening organization's information systems.
Course/Material License	Open Source

	Course #4
Partner Name	Vytautas Magnus University
Contact Person	Bronislovas Balvočius
Contact Email	bronislovas.balvocius@vdu.lt
Course(s) Name	IT Governance
ECTS Credits	6
Labs available	Yes
Completion	Credit + Written Exam
Description	Understanding IT governance and IT challenges. COBIT5, ITIL, ISO27001 and other IT governance and management frameworks and methodologies; IT governance objects and purpose – IT and business alignment, value creation, resource management, risk management, performance management, IT governance and management processes and process groups: Align, Plan, Organize; Build, Acquire, Implement; Deliver, Service, Support; Monitor and assure.
Learning Outcomes	Upon completion of this course, students will have knowledge and understanding of IT governance and management principles in companies and organizations, based on good management practices, frameworks and standards like COBIT, ITIL, ISO 27001. They will know IT governance objects and purpose – IT and business alignment, value creation, resource management, risk management, performance management, IT governance and management processes. Students will be capable of aligning IT function with main organization's functions, of applying IT governance and management good practices in own projects.
Course/Material License	Open Source

	Course #5
Partner Name	National College of Ireland
Contact Person	Michael Bradford
Contact Email	mbradford@ncirl.ie
Course(s) Name	Network Security and Penetration Testing
ECTS Credits	8
Labs available	Yes
Completion	CA 1:40% CA 2:60%
Description	The aim of the course is to critically assess network security concepts, attack vectors and mitigation solutions. Penetration testing methodologies and techniques will be applied to evaluate the security of network infrastructure and systems. The module enables learners to develop in depth knowledge and skills, both practical and critical, to successfully tackle technical challenges across the penetration testing scope. Emphasis is placed on practical skills, making use of the latest appropriate technology and techniques.
Learning Outcomes	Upon successful completion of this course, learners will be able to: - Critically assess network security characteristics and determine the scope of a penetration test of a network system. - Design, develop, and implement a security test on a network infrastructure. - Research and critically analyse network security vulnerabilities, as well as mitigation solutions. - Justify the choice of tools and techniques that are employed for penetration tests and evaluate the results of these tests.
Course/Material License	Not Open Source

	Course #6
Partner Name	National College of Ireland
Contact Person	Michael Bradford
Contact Email	mbradford@ncirl.ie
Course(s) Name	Security Fundamentals
ECTS Credits	8
Labs available	Yes
Completion	CA: 40% Terminal Exam: 60%
Description	This course aims to provide comprehensive, up-to-date, global common body of knowledge that ensures learners have a deep knowledge and understanding of new threats, technologies, regulations, standards, and practices to protect businesses from cyber-attacks. It starts by describing the current cyber landscape and potential threats. Then it delves into core security principles like confidentiality, integrity and availability to architect systems that provide key security characteristics. Commonly used frameworks and risk management methodologies are explored to address the suitability of appropriate controls. Various processes to operate in a resilient and secure environment are investigated to prevent and recover from any security incident while adhering to legal, regulatory and organizational requirements.
Learning Outcomes	Upon successful completion of this course, learners will be able to: - Compare and contrast new threats and technologies with respect to regulations, standards, and practices in order to protect businesses from cyber-attacks. - Research, evaluate and apply security management methodologies and best practices. - Compare and

	contrast security solutions for wired and wireless network - Devise and develop business continuity and disaster recovery plans. - Analyse and assemble responses from various Security Monitoring Systems.
Course/Material License	Not Open Source

	Course #7
Partner Name	National College of Ireland
Contact Person	Michael Bradford
Contact Email	mbradford@ncirl.ie
Course(s) Name	Forensics and eDiscovery
ECTS Credits	5
Labs available	Yes
Completion	CA 1:40% CA 2:60%
Description	This course aims to enable learners to develop a knowledge, skills and competence to approach a Digital Forensics investigation. This module also aims to develop skills associated with eDiscovery. Learners will gain practical experience in using various tools used in Windows forensics, Linux forensics, mobile forensics, network forensics and eDiscovery. This module provides an in-depth coverage of various sub-domains of digital forensics and how it is related to eDiscovery.
Learning Outcomes	"Upon successful completion of this course, learners will be able to: - Demonstrate in-depth critical awareness and interpretation of laws, compliance requirements, methods and procedures used in digital forensics investigations. - Carry out a forensic investigation of

	operating systems, mobile devices and networks, critically analyse the evidence and document the findings in a report. - Compare, evaluate and use forensic tools to forensically analyse digital devices. - Carry out an eDiscovery engagement across multiple platforms making use of various electronic discovery tools. - Critically analyse the results of an eDiscovery review, prepare production sets, write reports, and appraise the concepts for information retrieval and enterprise search technologies."
Course/Material License	Not Open Source

	Course #8
Partner Name	National College of Ireland
Contact Person	Michael Bradford
Contact Email	mbradford@ncirl.ie
Course(s) Name	Cloud Architectures and Security
ECTS Credits	8
Labs available	Yes
Completion	Project:40% Terminal Exam:60%
Description	This course aims to enable learners to investigate, critically analyse and assess security with respect to cloud computing. The module will address the key security concerns and challenges pertaining to developing, implementing, maintaining and utilising cloud computing systems and resources. In addition, learners will investigate and explore current techniques, methodologies, and architectural patterns and frameworks employed to manage security risks and policies. Learners will also develop strategies to identify, prevent,

	detect and recover from security breaches in cloud system environments. "
Learning Outcomes	"Upon successful completion of this course, learners will be able to: - Critically review computing systems security principles in order to assess how these principles relate to cloud computing environments. - Critically analyse the security challenges associated with cloud-based systems in order to identify and evaluate candidate cloud security architectures and deployment strategies. - Recommend solutions to detect, mitigate and prevent security breaches to the cloud-based systems. - Appraise security management models in order to develop security policies and processes for protecting the integrity of cloud-based systems."
Course/Material License	Not Open Source

	Course #9
Partner Name	National College of Ireland
Contact Person	Michael Bradford
Contact Email	mbradford@ncirl.ie
Course(s) Name	AI/ML in Cybersecurity
ECTS Credits	5
Labs available	Yes
Completion	Project:100%
Description	The objective of the AI/ML in Cybersecurity course is to endow learners with practical knowledge and skills on the application of artificial intelligence and machine learning techniques in cybersecurity. The module will also endow learners with

	foundational knowledge in data preparation processes such as: handling missing values, data cleaning, imbalanced data, data wrangling, etc. In undertaking this module, learners will gain hands on experience with a range of machine learning techniques for prediction, classification and clustering, problems using a variety of open cybersecurity datasets. Moreover, the module will look at different research trends, case studies and applications of AI and ML in cybersecurity industry solutions.
Learning Outcomes	Upon successful completion of this course, learners will be able to: - Critically analyse AI and machine learning techniques to assess best practice guidance and ethical implications when applied to specific cybersecurity problems. - Extract, clean and transform datasets in preparation for machine learning, and build evaluate machine learning models to extract knowledge from various cybersecurity datasets. - Critically review current AI and machine learning research and assess ethical considerations and research methods applied in the field. - Evaluate and utilise AI and machine learning technologies when designing and implementing cybersecurity solutions.
Course/Material License	Not Open Source

	Course #10
Partner Name	National College of Ireland
Contact Person	Michael Bradford
Contact Email	mbradford@ncirl.ie
Course(s) Name	Malware Analysis
ECTS Credits	5
Labs available	Yes

Completion	CA:50% Project:50%
Description	The aim of this course is to enable students to investigate different malware types and techniques, and the various tools used to identify, analyse, and defend against modern cybercrime attacks.
Learning Outcomes	Upon successful completion of this course, learners will be able to: - Research, compare, and contrast the different types of malwares. - Evaluate the Windows Operating System as a target platform for malicious code. - Investigate and assess malware through behavioural analysis and sandboxing. - Design, evaluate and implement defence solutions to prevent against malware attack. - Analyse criminal infrastructure as part of an online malware investigation.
Course/Material License	Not Open Source

	Course #11
Partner Name	National College of Ireland
Contact Person	Michael Bradford
Contact Email	mbradford@ncirl.ie
Course(s) Name	Business Resilience and Incident Management
ECTS Credits	5
Labs available	Yes
Completion	CA 1:40% CA 2:60%
Description	This course aims to provide learners with knowledge on documentation, strategies, and technologies that support the processes of business resilience and incident management. The module will examine how an organisation can prepare for business

	<p>disruption and what actions can be taken to prevent and contain an incident, reduce the impact to organisational systems and get the business operational as quickly as possible after an incident occurs. Learners will acquire the necessary incident management skills required to develop contextual plans, run books and the associated processes and tools to enable effective business resilience capabilities. Furthermore, learners will be able to identify and illustrate the challenges associated with developing risk-based BRIM processes. Learners will gain practical experience in aligning an organisation to industry standards and best practices that are commonly used for BRIM tasks with the domains of several stages, including preparation for incidents, detection and analysis of a security incident, containment, eradication, and full recovery, and post-incident analysis and learning. Learners will also develop practical skills associated with technical tools used at various stages of the IM process, including Firewalls, SIEM, NAC, WAF, AV, EDR and XDR etc.</p>
Learning Outcomes	<p>Upon successful completion of this module, learners will be able to:</p> <ul style="list-style-type: none"> - Evaluate incident response plans, their effectiveness and their alignment to industry leading standards and appropriate incident response principles and methodologies. - Critically appraise response activities for incident management from initial compromise to recovery and make recommendations for improvement. - Contrast methods to assess the maturity of an organisation's incident response capabilities. - Evaluate mechanisms to leverage blue team and the red team capabilities during an incident and appraise appropriateness and prioritisation for specific incident response use cases.
Course/Material License	Not Open Source

	Course #12
Partner Name	National College of Ireland
Contact Person	Michael Bradford
Contact Email	mbradford@ncirl.ie
Course(s) Name	IT Governance, Security and Ethics
ECTS Credits	6
Labs available	Yes
Completion	CA:40% Terminal Exam:60%
Description	The aim of the course is to present learners the bigger context in which an IT professional works, to introduce the learner to the IT governance and their role in the corporate governance, to present learner the relevant frameworks/standards used in IT and security governance and the relevant laws. The module also presents computer ethics, ethical issues in emerging fields in IT (e.g. ethics in AI), ethical code of conduct, aiming to stimulate students to build a high ethical and professional attitude. The module builds on top of Security Fundamentals and Development that covered significant elements of organizational security that links directly into IT and security governance.
Learning Outcomes	"Upon successful completion of this course, learners will be able to: - Describe and explain IT and security governance and discuss relevant frameworks. - Discuss a broad range of core policies, legal aspects in IT and security governance. - Discuss current models of information and computer ethics, relevant standards and current standardization efforts and evaluate the evolving nature of ethical norms relating to new technologies. "
Course/Material License	Not Open Source

	Course #13
Partner Name	Ataya
Contact Person	Georges Ataya & Nathan Minne
Contact Email	ga@atayapartners.com ; nm@atayapartners.com
Course(s) Name	Information Security Leadership (the CISO Fundamentals)
ECTS Credits	5
Labs available	Yes, physical
Completion	Performance evaluation
Description	<p>The core management activities of a modern information security leader include the security governance process, the risk management process, the program management process and the incident management process. This module will: cover the job description of a typical CISO today and where the CISO fits within the organisation including reporting lines and responsibilities, skills and expertise; talk about the typical challenges CISO's face in their role; address the design and implementation of an Information Security Strategy taking into account the assessment and handling of the relevant information security risks. Proper attention will be given to the application of the information security management system (ISMS) including proactive and reactive security incident management as well as tracking security leadership KPIs; focus on the (self-)evaluation of the CISO. Initial readings include the ISACA CISM body of knowledge, the ISO 27xxx security standards, the NIST Cybersecurity Framework, the ISACA Digital Trust approach, Hofstede cultural dimensions theory. The case study involves the development of a new security strategy as well as the improvement of the current security organisation via a business case towards top management.</p>

Learning Outcomes	Learn how to develop the landscape of the Information Security Function in terms of Actors (Board, CEO, C XO, Internal clients, CIO, regulators, assurance providers; external suppliers serving the business, external suppliers supporting information security activities); Requirements, deliverables and maturity of those actors. Learn how to develop department resources, skills, working methods, procedures. Learn how to define KPI/ dashboard and periodicity of reporting Learn how to build and maintain a Governance model, Information Security management framework/system. Learn how to define strategy, actions, activities, and programs/projects
Course/Material License	ITMA (Non Profit Association)

	Course #14
Partner Name	Ataya
Contact Person	Georges Ataya & Nathan Minne
Contact Email	ga@atayapartners.com ; nm@atayapartners.com
Course(s) Name	Security Controls Governance, Risk, Compliance and Certification
ECTS Credits	5
Labs available	Yes, physical
Completion	Performance evaluation
Description	"This module will take participants through the process of analysing context, defining scope, modelling threats, defining security controls and requirements, considering the solution space for controls, including technologies and operating models, and then finally evaluating risk (Inherent vs. Residual) and anchoring in policy, providing assurance that the controls operate as intended, e.g., for

	the purpose of internal or external assurance obligations or certification. This part builds on concepts introduced in module 1 (Information Security Leadership). Many concepts and approaches will be further elaborated in the next module (3, Security Architecture) through the lens of security by design. Readings include introductions into various control frameworks such as COBIT, ISO 27002, NIST cybersecurity controls, CIS20 and OWASP models. Some literature on threat modelling will also be provided. Case work will focus on the practical application of threat modelling techniques, control specification and governance definition and operation in an enterprise context focusing on a crown jewel. "
Learning Outcomes	Participants will gain a good understanding of security controls and their respective trade-offs from the angles of technology, people, and process. They will understand how kill-chain analysis in threat modelling helps bringing focus and cohesion and assists in building a business case. Finally, a layered approach at collection of assurance and reporting supports effective management of security controls.
Course/Material License	ITMA (Non Profit Association)

	Course #15
Partner Name	Ataya
Contact Person	Georges Ataya & Nathan Minne
Contact Email	ga@atayapartners.com ; nm@atayapartners.com
Course(s) Name	Security Architecture - Securing the Landscape
ECTS Credits	5
Labs available	Yes, physical
Completion	Performance evaluation

Description	"Often people talk about "security-by-design" or "privacy-by-design". Indeed, security cannot be "bolted on" at a later stage effectively. The better security is embedded "by design" in all layers of your organization's business, enterprise, and solution architecture and the better it is embedded in your design/delivery as well as run and operations, the better you will be able to understand your security posture and outstanding gaps and risks. To establish this understanding and the benefits, this module will demystify security architecture and previously listed domains and how it can and should be used not only by IT but can help to support governance, risk and compliance processes. "
Learning Outcomes	Various models will be studied by participants and how these can effectively be used to identify attacks vectors, threats and how these can be used to determine mitigating controls. Initial readings include the TOGAF, SABSA, and OSA frameworks. However, these will be completed with experienced speakers and concrete and practical cases.
Course/Material License	ITMA (Non Profit Association)

	Course #16
Partner Name	Ataya
Contact Person	Georges Ataya & Nathan Minne
Contact Email	ga@atayapartners.com ; nm@atayapartners.com
Course(s) Name	Security Operations: Continuity and Crisis Management
ECTS Credits	5
Labs available	Yes, physical
Completion	Performance evaluation

Description	<p>"This module will build upon the concepts of the previous modules where Information Security Governance, the Implementation of Security Controls, implementing a Secure Architecture are key building blocks to set up a qualitative Security Operations team. Information technology has become critical for most modern businesses that cyber risk has become a business risk. Security Operations teams are facing more pressure than ever to help manage this risk by identifying and responding to threats across a diverse set of technical assets, business processes, and users in a pro-active and reactive way. This module will learn how to design defences around the unique organizational requirements and its risk profile. We will give you the tools to build an intelligence-driven defence, measure progress towards your goals, and develop more advanced processes like threat hunting, active defence, and continuous Security Operations assessment.</p>
Learning Outcomes	<p>Participants will gain a good understanding of the core and auxiliary functions of a Security Operations team and the possible implementation models depending on the organization size and characteristics. The module will provide tools and frameworks for operational planning that will focus on key aspects like defence theory and mental models to understand and map potential adversaries, telemetry and analysis, attack detection and the investigative process, incident response and crisis communication up to assessment tools and frameworks to strive for continuous improvement. "</p>
Course/Material License	ITMA (Non Profit Association)

	Course #17
Partner Name	Ataya
Contact Person	Georges Ataya & Nathan Minne
Contact Email	ga@atayapartners.com ; nm@atayapartners.com

Course(s) Name	Cybersecurity Battleground: Threats, Vulnerabilities and Technologies
ECTS Credits	5
Labs available	Yes, physical
Completion	Performance evaluation
Description	"Cybersecurity management practices require the knowledge of own business, its functional and technical vulnerabilities and the threat landscape that needs to be addressed. The capabilities that require building cybersecurity capacity includes Identification, Protection, Detection, Response and Recovery techniques and processes. This module shall, based on the previous modules, address the day-to-day implementation of cybersecurity and information security, linking theories and practice. We will discuss how to link frameworks with business needs and risks in a day-to-day environment.
Learning Outcomes	This covers knowledge of existing frameworks, getting management buy-in, risk analysis, and the search for adequate solutions that are aligned with the risk appetite to the deployment and follow-up. Finally, we will give you some tools to help you function and think in adverse conditions and seemingly hostile environments. The case study involves the implementation of cybersecurity in a business environment where stakes are high and where board and company security knowledge limited."
Course/Material License	ITMA (Non Profit Association)

	Course #18
Partner Name	POLIMI
Contact Person	Paolo Trucco

Contact Email	paolo.trucco@polimi.it
Course(s) Name	Technology Risk Governance
ECTS Credits	5
Labs available	No
Completion	Minor Project + Written exam
Description	<p>"The course addresses all the relevant approaches, methods and models for supporting risk-informed decisions in managing complex socio-technical systems (e.g. technology selection, system design, management and governance) from business and institutional perspectives: - Risk governance of new and emerging technologies: Technology outlook and risk analysis methods for technology selection. Cases studies. - System Safety Engineering: Risk definition, modelling and reporting; Risk Engineering methods: Failure Mode Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Probabilistic Risk Analysis (PRA); FMECA and FTA Exercises. - Risk Analysis of Socio-Technical systems: Human and Organizational risk factors; Risk management of Organizational accidents (the Reason's model); the HRO (High Reliability Organization) theory. Critical incident analysis. - Organizational Resilience and Business Continuity Management (seminar in collaboration with the BCI). Guest speaker from industry. - Risk Governance of Complex Socio-Technical Systems: theory of Complex Adaptive Systems (CAS) and system-of-systems; Risk analysis of complex cyber-physical systems and networked infrastructure; Resilience Engineering of CAS. Discussion of cases from different industries. "</p>
Learning Outcomes	<p>" After successful completion of this course students will be able to: Identify and categorize technology risks of established and emerging technologies Describe and prioritize risk and resilience features of complex socio-technical systems exposed to cyber and physical threats Distinguish and compare approaches to and methods for</p>

	technology risk governance at different system life cycle stages Choose and applying the most appropriate risk assessment approach and methods given the key features of the complex socio-technical system at stake Examine and evaluate the suitability of an organization's technology risk governance model Prepare a strategic report on technology risk assessment."
Course/Material License	Not open source

	Course #19
Partner Name	CEFRIEL
Contact Person	Roberta Morici
Contact Email	roberta.morici@cefriel.com
Course(s) Name	Information Security Governance
ECTS Credits	3
Labs available	No
Completion	Performance evaluation
Description	"1 ISO 27001:2022 and IS Management System; 2 Cyber Risk Analysis and Management for Information Systems; 3 Management of security incidents;"
Learning Outcomes	"Understand and apply the principles of information security, including the implementation of a management system in compliance with ISO 27001:2022. Analyse and manage cyber risks for information systems using appropriate methodologies. Effectively manage cybersecurity incidents, ensuring operational continuity. Develop proactive strategies to prevent threats and protect informational assets. Evaluate the legal, ethical, and compliance

	implications of cybersecurity practices, communicating effectively with stakeholders."
Course/Material License	TBD

	Course #20
Partner Name	CEFRIEL
Contact Person	Roberta Morici
Contact Email	roberta.morici@cefriel.com
Course(s) Name	Cybercrime and Advanced Attack Tactics, Techniques and Technologies
ECTS Credits	3
Labs available	No
Completion	Performance evaluation
Description	"1 Vulnerability Assessment and Penetration Test; 2 Advanced security elements: an overview"
Learning Outcomes	"Analyse and understand advanced tactics, techniques, and technologies used in cybercrime, including their evolution and corresponding countermeasures. Conduct vulnerability assessments and penetration tests to identify and mitigate vulnerabilities in information systems. Examine advanced elements of cybersecurity, such as advanced encryption, endpoint protection, and advanced defence architectures. Evaluate new emerging threats in the cybercrime landscape and apply strategies to prevent, detect, and respond to advanced attacks. Integrate knowledge and techniques to analyse and understand investigative processes related to

	cybercrime, including the identification of digital evidence and tracking of attacks."
Course/Material License	TBD

	Course #21
Partner Name	CEFRIEL
Contact Person	Roberta Morici
Contact Email	roberta.morici@cefriel.com
Course(s) Name	Principles of Advanced Enterprise Security
ECTS Credits	3
Labs available	No
Completion	Performance evaluation
Description	"1 Third Party Cyber Risk Management; 2 Ethical Red Teaming, TIBER-EU; 3 Supply Chain Cybersecurity;"
Learning Outcomes	"Develop an understanding of third-party cyber risk management practices, including assessment methodologies and mitigation strategies. Gain proficiency in ethical red teaming methodologies, such as TIBER-EU (Threat Intelligence-Based Ethical Red Teaming for the European Union), to assess and improve organizational security posture. Explore supply chain cybersecurity concepts and techniques, including risk assessment, vendor management, and supply chain resilience strategies."
Course/Material License	TBD

	Course #22
Partner Name	CEFRIEL
Contact Person	Roberta Morici
Contact Email	roberta.morici@cefriel.com
Course(s) Name	The challenges for Information Security
ECTS Credits	3
Labs available	No
Completion	Performance evaluation
Description	"1 Security of IoT; 2 Mobile Malware, Security, e-Commerce, Mobile Payment"
Learning Outcomes	Explore the security considerations and best practices for Internet of Things (IoT) devices and ecosystems. Analyse the landscape of mobile malware, security concerns in e-commerce, and the security implications of mobile payment systems.
Course/Material License	TBD

	Course #23
Partner Name	CEFRIEL
Contact Person	Roberta Morici
Contact Email	roberta.morici@cefriel.com
Course(s) Name	Application, Accesses and Data in Security
ECTS Credits	3

Labs available	No
Completion	Performance evaluation
Description	"1 Security of web applications; 2 Security of legacy applications 3 Encryption, authentication and secure communications; 4 The evolution of Social Engineering, exposure and protection of digital identity, personal and corporate; 5 Human related attacks: tactics and defenses"
Learning Outcomes	"Understand the principles and best practices for securing web applications, including common vulnerabilities and mitigation strategies. Explore techniques for securing legacy applications to ensure continued protection of sensitive data and assets. Gain proficiency in encryption, authentication methods, and secure communication protocols to safeguard data integrity and confidentiality. Analyse the evolution of social engineering attacks and strategies for protecting digital identities, both personal and corporate, from exposure and exploitation. Evaluate tactics and defenses against human-related attacks, such as phishing and social engineering, to mitigate risks and enhance cybersecurity awareness."
Course/Material License	TBD

	Course #24
Partner Name	Munster Technological University
Contact Person	Triona McSweeney
Contact Email	triona.mcsweeney@mtu.ie
Course(s) Name	Security Architecture
ECTS Credits	8

Labs available	Yes
Completion	Multiple assessment types
Description	<p>Security Architecture is defined as a description, placement and allocation of security functions and controls with the aim of maintaining IT systems quality attributes such as confidentiality, integrity and availability. This module explores how an organisation can implement cybersecurity controls and organise its infrastructure best so that it can deter and respond to attacks when they occur. As part of this module security devices and products will also be explored in the context of their application as part of an overall security architecture implementation.</p>
Learning Outcomes	<p>1. Evaluate the applicability and use of Cybersecurity Architecture Frameworks to support and implement security features in an organisation. 2. Appraise the effectiveness of an organisation's Identity and Access Control (IAC) mechanisms. 3. Evaluate and secure a network through the appropriate design, placement and configuration of networking technologies, techniques and protocols. 4. Critically assess the security of a cloud based virtualised infrastructure with the aim of protecting data, application and services of cloud computing resources. 5. Appraise the application of cybersecurity controls and technologies used by an organisation to prevent an attack. 6. Appraise the application of cybersecurity controls and technologies used by an organisation to detect and respond to a successful attack. 7. Evaluate the security of an organisation from an Architecture viewpoint using each element of the Availability, Integrity, Confidentiality (AIC) Triad as a guide."</p>
Course/Material License	Not open source

	Course #25
Partner Name	Munster Technological University
Contact Person	Triona McSweeney

Contact Email	triona.mcsweeney@mtu.ie
Course(s) Name	Security Contingency Planning
ECTS Credits	5
Labs available	Yes
Completion	Multiple assessment types
Description	<p>Attacks on a company can cause severe damage in terms of lost revenue, reputation damage, network disturbances impacting not only the company themselves but also its customers. Developing a proper and well defined approach to contingency planning in the face of a cyber event reduces the impact of the damage so that the company can prepare for future cyber incidents. In this module students will learn about contingency planning and its main elements in incident response, disaster recovery and business continuity.</p>
Learning Outcomes	<p>1. Develop a business continuity plan through the effective identification of threats and analysing their impact on business operations. 2. Perform a threat assessment and modelling with the aim of optimising network security measures. 3. Develop a security awareness programme for an organisation with the aim of establishing a security conscious culture. 4. Critique a disaster recovery plan for efficacy and adherence to regulations and legal requirements. 5. Plan an incident response, backup, and recovery procedure for an organisation.</p>
Course/Material License	Not Open Source

	Course #26
--	-------------------

Partner Name	Munster Technological University
Contact Person	Triona McSweeney
Contact Email	triona.mcsweeney@mtu.ie
Course(s) Name	Security Management and Law
ECTS Credits	8
Labs available	Yes
Completion	Multiple assessment types
Description	This module examines national and EU laws, regulations and acts relevant to the field of cybersecurity and their impact in strengthening Ireland and the EU ability in tackling cybersecurity threats, attacks and cybercrime. In addition, this module will examine cybersecurity management frameworks and practices with the aim of improving an organisation's security posture and enhance resilience's against cyberattacks.
Learning Outcomes	1. Critically evaluate the laws and the relationship between laws with ethics in the domain of Information & Communication Technologies (ICT). 2. Evaluate national and international laws pertaining to cybercrime acts and their impact to individuals and organisations. 3. Assess the main issues relating to intellectual property and the intangible rights of ownership as it relates to software. 4. Analyse the main EU Data Protection Laws in relation to protecting EU citizens data and their respective security. 5. Critically evaluate security models and frameworks in their ability to serve as a roadmap to organise cybersecurity management activities in an organisation. 6. Evaluate security management practices in managing an organisations information assets in areas such as privacy, confidentiality, integrity and accountability. 7. Utilise project planning techniques and examine leadership styles within security management."
Course/Material License	TBD

	Course #27
Partner Name	Munster Technological University
Contact Person	Triona McSweeney
Contact Email	triona.mcsweeney@mtu.ie
Course(s) Name	Communications & Cybersecurity
ECTS Credits	5
Labs available	Yes
Completion	Multiple assessment types
Description	Students who complete this module will understand the importance of communication with particular focus on crisis communication related to technical and cyber challenges. The module explores how to manage internal communications and how to channel external communications to appropriate audiences. The tasks and processes carried out by the Cybersecurity team need to have management and employee buy in if they are to be successful. In particular, there often exists a disconnect between the languages spoken by cybersecurity professionals and a company's senior executives and board.
Learning Outcomes	1. Strategise internal and external communications in the context of emerging and ongoing cyber-security crises while managing engagement with the C-suite. 2. Develop internal communications plans that allow implementation of protocols in a speedy and effective manner. 3. Synthesise the ethical, business and social aspects of communicating technology-centred concepts for a non-technical audience while demonstrating understanding of cyber-security concepts. 4. Evaluate the overarching aspects of public relations (PR) for technology oriented businesses, reflecting the general principles of effective external communication. 5. Design the implementation of a communications crisis management plan that links internal and external communication conscious of cyber-contingency strategy within business needs."

Course/Material License	TBD
-------------------------	-----

	Course #28
Partner Name	UNIBS
Contact Person	Susanna Pozzolo
Contact Email	susanna.pozzolo@unibs.it
Course(s) Name	LAW AND DATA
ECTS Credits	5
Labs available	No
Completion	Written Exam
Description	<p>"The aim of the course is to provide a comprehensive overview of the European General Data Protection Regulation (GDPR), its principles, its rules, its method of implementation, its risk-based approach and the activity of the institutions it addresses. The analysis will focus on the pivotal concept of ""accountability"" of data controllers, the real keystone of the brand-new legal order on data protection, which specifically requires aware and responsible actors. The presentation of practical cases demonstrating the need to manage data protection compliance within a strict regulatory framework will allow students to practically develop an intuitive sensitivity to data protection compliance as one of the most valuable strategic assets of a company. Data governance consists of the ability to both extract and interpret salient information, but above all to be able to account for one's choices from the design of data processing, in order to minimise the risk of unnecessary or disruptive interference with personal data and privacy. Another objective of the course is to understand the different approaches to regulating data flows held by the EU's foreign trading partners and how the deep conceptual</p>

	distinction between 'privacy' and 'data protection' still influences them."
Learning Outcomes	<ul style="list-style-type: none"> - know the principles and concepts applicable to data ownership and processing; - follow continuous engineering innovation in data processing and understand the significant features of relevant technologies such as the application of big data and artificial intelligence technologies in different sectors; - master the tools and institutions compatible with the new legal framework governing data protection. <p>Application of knowledge:</p> <ul style="list-style-type: none"> - assess the impact of data processing on the rights and freedoms of data subjects; - elaborate and plan different privacy-by-design and privacy-by-default solutions depending on the specific purposes and situations of processing; - communicate and work effectively as an expert in data protection issues. <p>Judgement skills:</p> <p>At the end of the study programme, students will be able to:</p> <ul style="list-style-type: none"> - apply the rules set out in specific data processing schemes; - recognise the data protection risks within a processing operation and identify appropriate and effective measures to minimise them - prepare original reports and impact assessments of specific data processing simulations. <p>Communication skills:</p> <p>On completion of the programme of study, students will be able to:</p> <ul style="list-style-type: none"> - develop the ability to communicate in written form through exercises and in oral form through classroom interaction and debate; - use the knowledge and communication of data protection legislation; and - develop the ability to provide legal advice to data controllers and data processors. <p>Learning skills:</p> <p>At the end of the curriculum, students will be able to:</p> <ul style="list-style-type: none"> - build an analytical toolbox from data protection and privacy legislation; - solve problems in dynamic contexts and develop critical positions.
Course/Material License	TBD

	Course #29
Partner Name	UNSTPB
Contact Person	Răzvan Deaconescu
Contact Email	razvan.deaconescu@upb.ro
Course(s) Name	Computer and Network Security
ECTS Credits	5
Labs available	Yes
Completion	Credit + Written Exam
Description	"The course covers the issue of computer and network security, with an emphasis on application security, with a dual approach: the presentation of the system vulnerability discovery module and the exploitation of these vulnerabilities, followed by the presentation of systems and application security defense techniques. At the end of the course students will be able to: Recognize threats and vulnerabilities at the systems level, especially at the application memory level, Develops attack vectors for validating vulnerabilities and knowing the adversary's modus operandi, Assess the security level of an application, service, system, Propose solutions, libraries, applications, architectures to maximize the security of a computing system, Design and develop applications using secure programming techniques, This course will have an important practical component, which will entail: Investigating the security specifications of operating systems, applications and services Discovering security vulnerabilities through code auditing and reverse engineering techniques, Exploitation of security vulnerabilities, Using security techniques to protect your system and applications"
Learning Outcomes	"Identify and solve cybersecurity-related issues, Assess and manage technical vulnerabilities, Work on operating systems, servers, clouds and relevant infrastructures, Recognize threats and vulnerabilities at

	the systems level, especially at the application memory level, Develop attack vectors for validating vulnerabilities and knowing the adversary's modus operandi, Assess the security level of an application, service, system, Propose solutions, libraries, applications, architectures to maximize the security of a computing system, Design and develop applications using secure programming techniques Investigate the security specifications of operating systems, applications and services, Discoverer security vulnerabilities through code auditing and reverse engineering techniques, Exploitation of security vulnerabilities, Use security techniques to protect your system and applications "
Course/Material License	open source (CC by-SA)

	Course #30
Partner Name	UNSTPB
Contact Person	Răzvan Deaconescu
Contact Email	razvan.deaconescu@upb.ro
Course(s) Name	Applied Cryptography
ECTS Credits	5
Labs available	Yes
Completion	Credit + Written Exam
Description	"Knowledge of the fundamental elements of cryptography, as well as an understanding of the application of these concepts in particular applications, including those related to national security. Knowledge of the fundamental elements of cryptography. Knowledge of the weaknesses in existing and older cryptographic algorithms and implementations. Understanding the security of a cryptographic

	system. The ability to perform a security evaluation for a cryptographic system. Knowledge of the most popular cryptographic algorithms, both with symmetric and asymmetric keys. Understanding the functionality and security of some of the most popular cryptographic systems, such as TLS and EMV. "
Learning Outcomes	"Assess and manage technical vulnerabilities, Knowledge of cryptography basics Knowledge and security analysis of a cryptographic system, Knowledge of important security properties in Internet communication systems such as TLS, Understand security threats in secure communications, focusing on the necessary properties for end-to-end encryption systems such as Signal/Whatsapp. Understand limitations of security protocols in several examples, including the EMV payment system, Implement cryptographic protocols and applications Implement attacks on cryptographic protocols, Implement cryptographic algorithms for protection against adversaries ,Manipulate common cryptographic libraries in C and Python, Apply knowledge on popular applications and protocols "
Course/Material License	open source (CC by-SA)

	Course #31
Partner Name	UNSTPB
Contact Person	Răzvan Deaconescu
Contact Email	razvan.deaconescu@upb.ro
Course(s) Name	Cyberdefense and Cyberintelligence
ECTS Credits	5
Labs available	Yes

Completion	Credit + Written Exam
Description	<p>"The course aims to present and assimilate methodologies, tools and techniques for investigating and securing existing computer systems. The perspective through which the topics will be addressed is that of a security investigator or analyst, who, having dedicated tools and the necessary skills at his disposal, can discover vulnerabilities and defects in the infrastructure or applications used. Description and use of the main investigative techniques Identifying and fixing the main vulnerabilities of computing systems Assessing and improving security for computing systems Identifying the main sources of information for security Implementation of specific mechanisms to improve the security of computer systems Using specific utilities to determine the security of an application Inspect network traffic to determine security issues"</p>
Learning Outcomes	<p>"Identify and solve cybersecurity-related issues, Assess and manage technical vulnerabilities, Manage and analyse log files, Cooperate and share information with authorities and professional groups, Contribute to the development of the organisation's cybersecurity strategy, policy and procedures, Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders, Identify and assess cyber threat actors targeting the organisation, 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, 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 Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems Identification of threat</p>

	<p>landscape including attackers' profiles and estimation of attacks' potential, Understanding common cyber threats and attack vectors. Knowledge of encryption algorithms and cryptographic protocols. Familiarity with web application vulnerabilities such as SQL injection and cross-site scripting (XSS). Understanding of network protocols and communication technologies (e.g. TCP/IP, DNS). Awareness of endpoint security architectures and patterns Ability to configure and implement endpoint security solutions (e.g. anti-virus software, host-based firewalls). Proficiency in performing vulnerability assessments and penetration tests on web applications. Skills in configuring and managing network security devices (e.g. firewalls, intrusion detection systems). Ability to implement mobile device management (MDM) solutions to secure enterprise mobile devices. Proficiency in analyzing and responding to security incidents frameworks and incident response procedures."</p>
Course/Material License	open source (CC by-SA)

	Course #32
Partner Name	UNSTPB
Contact Person	Răzvan Deaconescu
Contact Email	razvan.deaconescu@upb.ro
Course(s) Name	Information Security Management
ECTS Credits	5
Labs available	Yes
Completion	Credit + Written Exam
Description	"The course covers organisation-level information security issues, implementation of an information security management system and

	<p>elements related to the information security audit. The course aims at training students for properly designing and implementing an information security management system, using nationally and internationally approved standards. The specific objectives of the course are: Knowing the elements necessary for designing and implementing an information security management system. Knowing the national / international standards regarding information security (ISO27k, COBIT, NIS Directive etc.). Implementation of an information security management system (ISMS) Knowing the main elements about cybersecurity and framework for improving it."</p>
Learning Outcomes	<p>"Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives 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 organisation, Ensure the organisation's resiliency to cyber incidents, Manage continuous capacity building within the organisation, 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 Define and apply maturity models for cybersecurity management Motivate and encourage people Identify cybersecurity needs of the organization Understand and apply regulations, best practices, standards in the field of cyber security, Manage aspects related to the internal structuring of an organization's resources to ensure an optimal level of cyber security, Establish an organization's cyber security plan, Organize resources to prevent and quickly react</p>

	to cyber security issues, Configure and maintain the organization's cyber security management systems"
Course/Material License	open source (CC by-SA)

	Course #33
Partner Name	UNSTPB
Contact Person	Răzvan Deaconescu
Contact Email	razvan.deaconescu@upb.ro
Course(s) Name	Operating Systems
ECTS Credits	5
Labs available	Yes
Completion	Credit + Written Exam
Description	<p>"The Operating Systems course helps you become a better software engineer/developer, regardless of the programming language and platform used. After this course you will develop your meta-technical skills (working on large projects, teamwork) in parallel with acquiring technical skills and knowledge (understanding the software stack, using low-level programming interfaces). On the part of the course, you will understand how practical applications are influenced by the components of the software stack, with an emphasis on low-level components. On the lab side you will see how once a concept is understood, it can be used in any programming language, and you will understand an already developed application, perform measurements and evaluations and extend applications. On the homework side, you will develop both applications from scratch and starting from code written by others and you will evaluate them (performance, robustness, security). We will insist on the skills of a</p>

	good software engineer / developer, skills that develop and improve continuously: understanding the code written by others, auditing the code, developing quality code that contains as few software defects as possible, good working practices at collaborative software projects."
Learning Outcomes	"Assess and manage technical vulnerabilities Work on operating systems, servers, clouds and relevant infrastructures. Manage and analyse log files. Use low-level interfaces from the software stack for the development of high-performance, robust, secure applications. Understand the performance and design trade-offs in complex software systems. Understand code written by others, auditing code. Understand the API exposed by a software component, its proper use. Develop high quality code that contains as few software defects as possible. Gain good working practices on collaborative software projects Evaluate and improve code written by you or others. Work on large software projects: going through the code, reading the documentation, expanding the project. Work in teams. Improve existing applications, with respect to security, performance, efficiency. Understand the software stack of a computing system, the role of each part of the software stack: the role of the operating system, its subsystems and low-level software components for the development, maintenance and improvement of applications. Investigate software components to detect performance problems (bottlenecks), to discover software defects and vulnerabilities, to understand their operation within the system"
Course/Material License	open source (CC by-SA)

	Course #34
Partner Name	MRU
Contact Person	Marius Laurinaitis

Contact Email	laurinaitis@mruni.eu
Course(s) Name	Fundamental Principles and Risk Management of Cybersecurity
ECTS Credits	6
Labs available	No
Completion	Exam
Description	"Concept of cyber security. Types and models of cyber-attacks. Taxonomy of the incidents. Social engineering and most popular attack vectors. Evolution of cyber threats and analysis of well-known cases; Concept of the risk assessment and practical application. Information technologies and their influence on daily operations Assessment of cyber threats; Best practice in the field of cyber security solutions. Security standards and critical controls; Preparing the risk assessment."
Learning Outcomes	Analyse and consolidate organisation's quality and risk management practices. Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards Learn to conduct ethical hacking Evaluate cybersecurity risks and maturity models
Course/Material License	TBD

	Course #35
Partner Name	MRU
Contact Person	Marius Laurinaitis
Contact Email	laurinaitis@mruni.eu

Course(s) Name	Security Economics
ECTS Credits	4
Labs available	No
Completion	Credit and written Exam
Description	"Economics and the cyber security, concepts and practice. Case studies; Cyber security incidents and the effect on organisation operations. Analysis of technical reports. Defining the indicators of compromise; Information technologies and their role in the security incidents. Forensics and the analysis of data."
Learning Outcomes	Identify and solve cybersecurity-related issues Assess the security and performance of solutions Know about multidiscipline aspect of cybersecurity, Cyber threats and cyber trends
Course/Material License	TBD

	Course #36
Partner Name	MRU
Contact Person	Marius Laurinaitis
Contact Email	laurinaitis@mruni.eu
Course(s) Name	Organisational Cyber Security Culture
ECTS Credits	6
Labs available	No
Completion	Credit and written Exam

Description	"The concept of cyber culture in an organization; The need for cyber culture / The role / importance of cyber culture in cyber security; Understanding the process of change in cyber culture; Elements of planning / forming a cyber culture program; Cyber culture implementation cycle / detailed stages."
Learning Outcomes	Implement cybersecurity recommendations and best practices Acknowledge human aspects of security and privacy Cybersecurity awareness, education and training programme development
Course/Material License	TBD

	Course #37
Partner Name	MRU
Contact Person	Marius Laurinaitis
Contact Email	laurinaitis@mruni.eu
Course(s) Name	Management of IT Projects
ECTS Credits	6
Labs available	No
Completion	Credit + Exam
Description	"Projects and project management – concepts, standards, and methodologies. IT project specific issues. Public and private sector IT project specifics. Types of IT projects. Project Manager; IT projects context: project life cycle project, interested parties and the organizational environment. IT project management context: programmes, projects, portfolios, project management unit, sub-projects and projects chain; Project processes. Initiating and planning

	the project. The integration of project management. The volume of projects management, work breakdown structure. Project time management, project schedules and its preparation; Project costs, the preparation of the budget; Human resource management."
Learning Outcomes	Human resource management Human aspects of security and privacy Cybersecurity resource management
Course/Material License	TBD

	Course #38
Partner Name	New Course
Contact Person	TBD
Contact Email	TBD
Course(s) Name	NEW - Training Cybersecurity - The foundations of didactics I
ECTS Credits	5
Labs available	No
Completion	Credit + Exam
Description	didactic principles of adult learning, implementation and assessment of training sequences, brief seminars and group discussions, understanding the benefit of security-conscious people implementing additional defences as well as cybersecurity risks posed by people, assisting employers to actively enhance security through training, foundations of human risk management
Learning Outcomes	1. Analyse the design of their courses. 2. Create a lesson plan based on the didactic principles of adult learning. 3. Define suitable course

	objectives. 4. Apply various tools and training methods. 5. Reflect and continuously develop their training skills.
Course/Material License	NEW – not yet

	Course #39
Partner Name	TBD
Contact Person	TBD
Contact Email	TBD
Course(s) Name	NEW – Cybersecurity Auditing
ECTS Credits	5
Labs available	No
Completion	TBD
Description	This course prepares students to conduct auditing processes with regards to the efficiency of an organization`s cybersecurity environment and it`s compliance with frameworks and best practices.
Learning Outcomes	<p>LO1 Students are able to analyse business processes and review software and hardware security.</p> <p>LO2 Students apply auditing tools with integrity and collect and evaluate auditing information.</p> <p>LO3 Students are familiar with auditing standards, methodologies and frameworks.</p> <p>LO4 Students are familiar with legal and regulatory requirements and best practices.</p>

Course/Material License	Open Source
-------------------------	-------------

	Course #40
Partner Name	New Course
Contact Person	TBD
Contact Email	TBD
Course(s) Name	NEW - Training Cybersecurity - The foundations of didactics II
ECTS Credits	5
Labs available	No
Completion	Credit + Exam
Description	The course offers a comprehensive exploration of pedagogical principles, content adaptation, active learning methods, teaching strategies, and real-world integration, ensuring educators are equipped to deliver engaging and effective instruction. Emphasizing critical thinking, collaboration, and ethical considerations, the course provides educators with the tools to foster student engagement and prepare them for the challenges of the cybersecurity field. Through assessment and feedback strategies, educators learn to support student learning and growth while continuously developing their own professional skills and staying abreast of emerging trends and best practices in cybersecurity education.
Learning Outcomes	1. Understanding of Pedagogical Principles (relevant to teaching cybersecurity, including instructional design, learning styles, and assessment strategies) 2. Adaptation of Content (to different learning environments, student backgrounds, and educational levels, ensuring relevance and engagement). 3. Integration of Active Learning Methods: Explore and implement various active

	<p>learning methods, such as case studies, simulations, hands-on exercises, and group discussions</p> <p>4. Development of Effective Teaching Strategies.</p> <p>5. Integration of Real-world Scenarios</p> <p>6. Promotion of Critical Thinking Skills.</p> <p>7. Assessment and Feedback Strategies,</p> <p>8. Ethical and Legal Considerations (including responsible conduct of research, ethical hacking principles, and compliance with relevant laws and regulations)</p> <p>9. Professional Development (by staying updated on emerging trends)</p>
Course/Material License	NEW – not yet

	Course #41
Partner Name	TBD
Contact Person	TBD
Contact Email	
Course(s) Name	NEW - Cybersecurity in Emerging Technologies
ECTS Credits	5
Labs available	YES
Completion	TBD
Description	<p>These module aims to prepare students to navigate the dynamic landscape of cybersecurity by equipping them with the knowledge, skills, and mindset necessary to leverage emerging technologies effectively while addressing associated challenges and risks. It combines ethical and legal considerations with the assessment of security implications and the evaluation of security solutions. Further</p>

	students explore emerging technologies such as AI, ML and IoT and their integration into security frameworks.
Learning Outcomes	<p>1. Understanding Emerging Technologies: such as artificial intelligence (AI), machine learning, blockchain, Internet of Things (IoT), and quantum computing. 2. Assessment of Security Implications: Analyse the security implications of emerging technologies, including vulnerabilities, threats, and risks, and evaluate strategies for mitigating these risks to ensure robust cybersecurity posture. 3. Integration into Security Frameworks: to enhance threat detection, incident response, and overall security effectiveness. 4. Evaluation of Security Solutions: leveraging emerging technologies, such as AI-based threat detection systems, blockchain for secure data management, or IoT security protocols, considering factors like performance, scalability, and cost-effectiveness. 5. Hands-on Experience: Gain practical experience through hands-on labs, simulations, or projects that allow students to experiment with and implement emerging cybersecurity technologies in simulated environments. 6. Ethical and Legal Considerations/ 7. Adaptation to Evolving Threat Landscape: Understand how emerging technologies can be leveraged by both attackers and defenders in the constantly evolving cybersecurity threat landscape, and develop strategies to stay ahead of emerging threats. 8. Collaboration and Interdisciplinary Perspectives, 9. Communication of Complex Concepts, 10. Continuous Learning and Adaptation</p>
Course/Material License	TBD

	Course #42
Partner Name	TBD
Contact Person	TBD
Contact Email	
Course(s) Name	NEW - Research project and Master's Thesis
ECTS Credits	15

Labs available	TBD
Completion	TBD
Description	Writing a thesis allows students to delve deeply into a specific area of cybersecurity, to independently develop a technical project and gain in-depth knowledge and expertise. Through rigorous research and analysis, students develop critical thinking, problem-solving, and technical skills essential for success in the field. Completing a thesis demonstrates a student's ability to undertake independent research and communicate findings effectively, enhancing their credibility and opening doors to career opportunities in academia, industry, or government.
Learning Outcomes	1. In-depth Understanding of a specific topic or area within cybersecurity through extensive research and analysis. 2. Research Skills: including literature review, data collection, analysis, and interpretation, to investigate relevant cybersecurity issues or challenges. 3. Critical Thinking: to evaluate existing cybersecurity theories, methodologies, and practices, and propose innovative solutions or approaches. 4. Problem-Solving Abilities: by identifying cybersecurity problems, analysing their root causes, and developing effective strategies or solutions. 5. Technical Expertise: Deepen technical expertise depending on the focus of the thesis. 6. Communication Skills: Enhance communication skills through the clear and effective presentation of research findings, methodologies, and conclusions in a technical report and oral defense. 7. Ethical Considerations: Understand and adhere to ethical considerations in cybersecurity research, including privacy, confidentiality, integrity, and responsible conduct of research.
Course/Material License	NEW COURSE – NOT YET

	Course #43
Partner Name	TBD
Contact Person	TBD

Contact Email	
Course(s) Name	NEW - Industry Internship
ECTS Credits	10
Labs available	TBD
Completion	TBD
Description	This industry internship offers students invaluable practical experience, networking opportunities, and skill development. It provides insights into industry practices, enhances resumes, and fosters professional growth through feedback and learning opportunities. Internships also allow students to explore various career paths within cybersecurity management, assess organizational culture, and build confidence in their abilities. This internship serves as a crucial bridge between academic learning and real-world practice, equipping students with the knowledge, skills, and experience needed for success in the cybersecurity field.
Learning Outcomes	"1. Hands-on Experience: Gain practical, real-world experience in cybersecurity practices, tools, and techniques within a professional environment. 2. Application of Knowledge, 3. Technical Skills Development: in areas such as network security, cryptography, penetration testing, malware analysis, incident response, and secure coding. 4. Problem-Solving Skills: by tackling complex cybersecurity issues, identifying vulnerabilities, and implementing effective solutions. 5. Communication Skills: effectively conveying technical information, discussing cybersecurity strategies with colleagues, and presenting findings to stakeholders, 6. Teamwork and Collaboration, 7. Adaptability and Resilience, 8. Ethical and Legal Awareness, 9. Work Ethic and Continuous Learning"
Course/Material License	Not open source

Further courses to be considered in further developed curriculum:

	Course #44
Partner Name	UNSTPB
Contact Person	Florin Anton
Contact Email	florin.anton@upb.ro
Course(s) Name	Network and Systems Security*
ECTS Credits	5
Labs available	Yes
Completion	Credit + Written Exam
Description	In the current context, IT security is one of the key points that an organization must take into account, and the education and awareness part is fundamental to develop a human resource that will be an active part of the security component. The Network and Systems Security discipline is a fundamental discipline for future employees in fields of activity that fall within the area of information technology, developing theoretical and practical skills regarding computer security in organizations, security standards and technologies, policies and procedures, principles of security, cryptography, public key infrastructure, secure software development, disaster recovery, etc.
Learning Outcomes	"Identify and solve cybersecurity-related issues, Work on operating systems, servers, clouds and relevant infrastructures. Manage and analyse log files. List the main security models and their characteristics. Classifies the types of security threats. Understands and applies auditing modes. Uses the public key infrastructure, functioning of the authentication, authorization and accounting protocols. Defines disaster recovery and business continuity plans. Identifies risks and catalogues them. Works productively in a team.

	Elaborates a scientific text. Experimentally verifies identified solutions."
Course/Material License	open source (CC by-SA)

	Course #45
Partner Name	Universidad Internacional de la Rioja
Contact Person	Sergio Mauricio Martínez Monterrubio
Contact Email	sergiomauricio.martinez@unir.net
Course(s) Name	Network Security and Intelligent Threat Analysis
ECTS Credits	5
Labs available	Yes
Completion	credit
Description	"The purpose of this course is to describe the protection technologies for distributed information systems. Computer networks, mainly based on communications over the TCP/IP protocol, inherit many of the security features of this protocol. This is the first objective of the course, from these bases the vulnerabilities and threats of networked information systems are presented, and then, in contrast, the most common security protocols for their protection are presented. The course also pays special attention to system protection topologies based on firewalls. Subsequently, it focuses on

	the proactive protection of systems, describing protection strategies based on decoys, intrusion detection and protection systems and security event management systems (SIEM). All these aspects are highly topical since these types of safeguards are the main protection against active persistent threats (known as APT, Advanced Persistent Threat). In the last part of the course, a review of the fundamental concepts of cryptography applied to network security is presented: symmetric and asymmetric encryption algorithms, digital signature, message authentication and summary functions. With this knowledge it is possible to approach in depth the study of secure protocols both in wired networks (MACsec, IPSec, SSL/TLS and DNSsec) and in wireless networks (WEP, WPA, WPA2 and WPA3)."
Learning Outcomes	Not disclosed by partner
Course/Material License	Not disclosed by partner

	Course #46
Partner Name	Universidad Internacional de la Rioja
Contact Person	Sergio Mauricio Martínez Monterrubio
Contact Email	sergiomauricio.martinez@unir.net
Course(s) Name	Security in Systems, Applications and Big Data
ECTS Credits	5
Labs available	Yes
Completion	credit
Description	"This course studies the measures or activities that are necessary to implement the security of operating systems and web applications so

	that once deployed online, they behave as expected, both by the owners and by the users of the application and can mitigate any attack. In addition, it delves into the security of services deployed in cloud architectures and big data. The basis of the security of online applications and services deployed in the cloud depends on the security of the operating systems that support them installed on physical machines, virtualized or in containers. It is critical to address the security activities performed before and after systems and applications are deployed by following a Secure Software Development Life Cycle (SSCLC). An SSDLC involves the performance of certain security activities related to security requirements, secure design and development, as well as security testing and operations that must be carried out in an orderly and procedural manner by security expert personnel. The architectures and services that support massive data computation in the Cloud are an example of a particular architecture that is considered necessary to address due to its proliferation and boom in recent times. A concrete open source case study and the possibilities offered by the market for security design and implementation will be analysed."
Learning Outcomes	Not disclosed by partner
Course/Material License	Not disclosed by partner

	Course #47
Partner Name	Universidad Internacional de la Rioja
Contact Person	Fidel Paniagua Diez
Contact Email	fidel.paniagua@unir.net
Course(s) Name	Ethical Hacking and Malware Analysis

ECTS Credits	5
Labs available	Yes
Completion	credit
Description	<p>"In this course, the student will learn the steps and mechanisms necessary to complete a cyber-attack, as well as how to mitigate them. For this, all the steps of a pentesting will be included to follow the current guidelines and methodologies that will reinforce us in obtaining such information. Students will be introduced to the concepts related to "Malware Analysis", necessary to guide their future learning and future activities related to this sector of cybersecurity. This discipline provides the ability to analyse and understand the operation of malicious code (such as Trojans, viruses, rootkits, etc.), in order to assess the damage caused, design technical measures for its defence and assess the intentions and capabilities of an attacker. At the end of this course, the student will be able to: Understand the concept of vulnerability with its typology and know how to analyse all types of vulnerabilities. Obtain information for the generation of own attack vectors. Use and understand exploitation mechanisms and tools that automate them. Obtain knowledge of post-exploitation mechanisms once vulnerable systems have been compromised. Know and know how to apply the main standards, methodologies, tools and best practices of pentesting. To be introduced to the different techniques, methods and methodologies of malware analysis. To know the different tools used in the various malware analysis techniques. To study the implementation of a secure malware analysis laboratory in order to avoid malware evasion accidents."</p>
Learning Outcomes	Not disclosed by partner
Course/Material License	Not disclosed by partner

	Course #48
Partner Name	UNIRI
Contact Person	Tomislav Slaviček-Car
Contact Email	tomislav.slavicekcar@uniri.hr
Course(s) Name	Automation of Security Tasks
ECTS Credits	6
Labs available	YES
Completion	Written Exam or Project
Description	<p>"1. Introduction to Python Programming</p> <ul style="list-style-type: none"> - Basic syntax, data types, and control structures - Functions, modules, and packages <p>2. Python Scripting for Cybersecurity Automation</p> <ul style="list-style-type: none"> - Network scanning and enumeration - Vulnerability assessment and exploitation - Log analysis and monitoring <p>3. Data Manipulation and Analysis in Python</p> <ul style="list-style-type: none"> - Introduction to Pandas and NumPy - Data cleaning, transformation, and analysis techniques <p>4. Cyber Threat Intelligence Fundamentals</p>

	<ul style="list-style-type: none"> - Overview of Cyber Threat Intelligence (CTI) lifecycle - Role of CTI in proactive cybersecurity defense <p>5. Python for Threat Intelligence Gathering</p> <ul style="list-style-type: none"> - Web scraping and data extraction techniques - Integration with threat intelligence platforms (TIPs) <p>6. Automation for Threat Detection and Response</p> <ul style="list-style-type: none"> - Designing automated detection and response workflows - Utilizing Python for incident response automation <p>7. Secure Coding Practices in Python</p> <ul style="list-style-type: none"> - Handling sensitive data securely - Input validation and sanitization - Secure file handling and communication protocols"
Learning Outcomes	<p>"1. Master Python Fundamentals: - Understand basic Python syntax, data types, and control structures. - Demonstrate proficiency in functions, modules, and packages in Python.</p> <p>2. Apply Python for Cybersecurity Tasks: - Develop Python scripts for automating common cybersecurity tasks, such as network scanning, vulnerability assessment, and log analysis. - Utilize Python libraries/frameworks like Scapy, Nmap, Requests, and BeautifulSoup for various cybersecurity applications.</p> <p>3. Implement Data Manipulation and Analysis: - Use Python libraries like Pandas and NumPy for data manipulation and analysis in cybersecurity scenarios, such as analyzing logs, extracting indicators of compromise (IOCs), and correlating data.</p> <p>4. Explore Cyber Threat Intelligence Concepts: - Understand the role of Cyber Threat Intelligence (CTI) in cybersecurity operations.</p> <ul style="list-style-type: none"> - Familiarize with the ENISA Cyber Threat Intelligence Specialist role and its responsibilities. <p>5. Develop Threat Intelligence Gathering Scripts:</p>

	<ul style="list-style-type: none"> - Design Python scripts to gather threat intelligence from various sources, including open-source intelligence (OSINT) feeds, social media, and dark web forums. <p>6. Implement Automation for Threat Detection:</p> <ul style="list-style-type: none"> - Develop Python scripts to automate the detection of suspicious activities, anomalies, and potential threats within network traffic and system logs. <p>7. Practice Secure Coding and Scripting:</p> <ul style="list-style-type: none"> - Apply secure coding practices in Python to mitigate common vulnerabilities and ensure the reliability and integrity of cybersecurity scripts and tools."
Course/Material License	New course – not yet designed

	Course #49
Partner Name	UNIBS
Contact Person	Giorgio Pedrazzi
Contact Email	giorgio.pedrazzi@unibs.it
Course(s) Name	NEW - Diversity, Equity and Inclusion in Cybersecurity
ECTS Credits	3
Labs available	No
Completion	Written Exam or project
Description	"In this course, the student will learn how inclusion and diversity can leverage the work of cybersecurity teams in organisational and institutional contexts. In doing so, the student will be accompanied to to understand the importance of inclusive practices and diversity in cybersecurity teams, policy-making, and compliance strategies

	<p>and to identify ways to promote diversity and inclusion in such contexts.</p> <p>The course will provide a practical approach to this broad topic so that the student can develop policies and frameworks to enforce ethical practices, promote diversity, and ensure compliance in various organizational settings.</p> <p>Aligning to the practices of major international cybersecurity institutions, the student will also learn how to build and sustain a diverse, inclusive, multicultural and skilled cybersecurity workforce."</p>
Learning Outcomes	<p>"a) Promote Inclusion and Diversity: Understand the importance of inclusive practices and diversity in cybersecurity teams, policy-making, and compliance strategies.</p> <p>b) Develop Policies and Frameworks: Learn to create and implement policies that enforce ethical practices, promote diversity, and ensure compliance in various organizational settings."</p>
Course/Material License	new course – not yet designed

	Course #50
Partner Name	UNIBS
Contact Person	Giorgio Pedrazzi
Contact Email	giorgio.pedrazzi@unibs.it
Course(s) Name	NEW – Cyber Ethics
ECTS Credits	6
Labs available	No
Completion	Written exam

Description	<p>"By exploring the ethical theories and principles that underpin decision-making in cybersecurity, this course aims to provide the students with an overview on ethics and responsibility challenges connected to digital environments, organizations and people.</p> <p>This course will analyze real-world cybersecurity challenges using ethical frameworks and will develop solutions that adhere to high ethical standards as well as that applies ethical practices in cybersecurity.</p> <p>This course will be managed by UNIBS and could be involve other partners fond of the suggested topics."</p>
Learning Outcomes	<p>"a) Understand Ethical Foundations: Explore the ethical theories and principles that underpin decision-making in cybersecurity.</p> <p>b) Apply Ethical Practices in Cybersecurity: Analyze real-world cybersecurity challenges using ethical frameworks and develop solutions that adhere to high ethical standards."</p>
Course/Material License	new course – not yet designed

Recommended Curriculum: CISO

Work Package 2, Task 2.2



Your Curriculum

Year	Winter semester	Summer semester	Credits
1st	Cybersecurity Battleground: Threats, Vulnerabilities and Technologies		56
	Information Security Governance	Security Controls Governance, Risk, Compliance and Certification	
	Security Fundamentals	Information Security Leadership (the CISO Fundamentals)	
	Fundamental Principles and Risk Management of Cybersecurity	Technology Risk Governance	
	Information System Security	Cloud Architectures and Security	
	Communications & Cybersecurity		
2nd		Business Resilience and Incident Management	74
	Foundations of Cryptography	Security Architecture Securing the Landscape	
	Information Security Management	Cybercrime and Cybersecurity	
	Security Management and Law	Management of IT Projects	
	The challenges for Information Security	Thesis	
	Security Architecture	Practice in Company	
3rd			0
Total Credits			130

List of Courses

Name	Type	Semester	ETCS Credits	Training
Business Resilience and Incident Management	mandatory	summer	5	Yes
Cloud Architectures and Security	mandatory	summer	8	Yes
Communications & Cybersecurity	voluntary	winter	5	No
Cybercrime and Cybersecurity	mandatory	summer	3	No
Cybersecurity Battleground: Threats, Vulnerabilities and Technologies	mandatory	winter	5	Yes
Foundations of Cryptography	voluntary	winter	6	Yes
Fundamental Principles and Risk Management of Cybersecurity	voluntary	winter	6	No
Information Security Governance	voluntary	winter	3	Yes
Information Security Leadership (the CISO Fundamentals)	mandatory	summer	5	Yes
Information Security Management	mandatory	winter	5	No
Information System Security	mandatory	winter	6	Yes
Management of IT Projects	voluntary	summer	6	No
Practice in Company	voluntary	summer	10	Yes
Security Architecture	voluntary	winter	8	Yes
Security Architecture Securing the Landscape	mandatory	summer	5	Yes
Security Controls Governance, Risk, Compliance and Certification	voluntary	summer	5	Yes
Security Fundamentals	mandatory	winter	8	Yes
Security Management and Law	voluntary	winter	8	No
Technology Risk Governance	mandatory	summer	5	No
The challenges for Information Security	mandatory	winter	3	No
Thesis	mandatory	summer	15	No

ECSF Profiles

Profile	Supported	ECTS*
Chief Information Security Officer (Ciso)	Yes	38.51
Cyber Incident Responder	No	-
Cyber Legal, Policy & Compliance Officer	Yes	11.58
Cyber Threat Intelligence Specialist	No	-
Cybersecurity Architect	No	-
Cybersecurity Auditor	No	-
Cybersecurity Educator	No	-
Cybersecurity Implementer	No	-
Cybersecurity Researcher	Yes	15.49
Cybersecurity Risk Manager	Yes	28.83
Digital Forensics Investigator	No	-
Penetration Tester	No	-

*decimal numbers in ECTS result from single courses aiming at more than one ENISA ECSF profile.

Supported ECSF Skills

- Analyse and comply with cybersecurity-related laws, regulations and legislations
- Analyse and consolidate organisation's quality and risk management practices
- Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks
- Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls
- Anticipate cybersecurity threats, needs and upcoming challenges
- Anticipate required changes to the organisation's information security strategy and formulate new plans
- Apply auditing tools and techniques
- Assess and enhance an organisation's cybersecurity posture
- Assess the security and performance of solutions
- Automate threat intelligence management procedures
- Build a cybersecurity risk-aware environment
- Build resilience against points of failure across the architecture
- Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy
- Collaborate with other team members and colleagues
- Collect, analyse and correlate cyber threat information originating from multiple sources
- Communicate, coordinate and cooperate with internal and external stakeholders
- Communicate, explain and adapt legal and regulatory requirements and business needs
- Communicate, present and report to relevant stakeholders

Communicate, present and report to relevant stakeholders

- Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements
- Conduct ethical hacking
- Conduct technical analysis and reporting
- Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools
- Coordinate the integration of security solutions
- Decompose and analyse systems to develop security and privacy requirements and identify effective solutions
- Decompose and analyse systems to identify weaknesses and ineffective controls
- Define and apply maturity models for cybersecurity management
- Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles
- Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing
- Develop and communicate, detailed and reasoned investigation reports
- Develop, champion and lead the execution of a cybersecurity strategy
- Draw cybersecurity architectural and functional specifications
- Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks
- Establish a cybersecurity plan
- Explain and communicate data protection and privacy topics to stakeholders and users
- Explain and present digital evidence in a simple, straightforward and easy to understand way
- Follow and practice auditing frameworks, standards and methodologies
- Generate new ideas and transfer theory into practice
- Guide and communicate with implementers and IT/OT personnel
- Identify and select appropriate pedagogical approaches for the intended audience
- Identify and solve cybersecurity-related issues
- Identify non-cyber events with implications on cyber-related activities
- Identify threat actors TTPs and campaigns
- Implement cybersecurity recommendations and best practices
- Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards
- Influence an organisation's cybersecurity culture
- Integrate cybersecurity solutions to the organisation's infrastructure
- 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
- Manage cybersecurity resources
- Model threats, actors and TTPs
- Monitor new advancements in cybersecurity-related technologies
- Motivate and encourage people
- Practice all technical, functional and operational aspects of cybersecurity incident handling and response
- Propose and manage risk-sharing options
- Propose cybersecurity architectures based on stakeholder's needs and budget
- Provide training towards cybersecurity and data protection professional certifications
- Review and enhance security documents, reports, SLAs and ensure the security objectives
- Select appropriate specifications, procedures and controls
- Think creatively and outside the box
- Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies
- Understand, practice and adhere to ethical requirements and standards

... ..

- Use and apply CII platforms and tools
- Utilise existing cybersecurity-related training resources
- Work ethically and independently; not influenced and biased by internal or external actors
- Work on operating systems, servers, clouds and relevant infrastructures
- Work under pressure

Supported ECSF Knowledge

- Auditing standards, methodologies and frameworks
- Computer networks security
- Computer Security Incident Response Teams (CSIRTs) operation
- Computer systems vulnerabilities
- Conformity assessment standards, methodologies and frameworks
- Criminal investigation procedures, standards, methodologies and frameworks
- Cross-domain and border-domain knowledge related to cybersecurity
- Cyber threat actors
- Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks
- Cyber threats
- Cybersecurity attack procedures
- Cybersecurity controls and solutions
- Cybersecurity maturity models
- Cybersecurity policies
- Cybersecurity procedures
- Cybersecurity recommendations and best practices
- Cybersecurity related laws, regulations and legislations
- Cybersecurity risks
- Cybersecurity standards, methodologies and frameworks
- Cybersecurity trends
- Cybersecurity-related certifications
- Cybersecurity-related requirements analysis
- Cybersecurity-related research, development and innovation (RDI)
- Cybersecurity-related technologies
- Digital forensics analysis procedures
- Digital forensics recommendations and best practices
- Digital forensics standards, methodologies and frameworks
- Ethical cybersecurity organisation requirements
- Incident handling communication procedures
- Incident handling recommendations and best practices
- Incident handling standards, methodologies and frameworks
- Incident handling tools
- Legacy cybersecurity procedures
- Legal, regulatory and legislative compliance requirements, recommendations and best practices
- Legal, regulatory and legislative requirements on releasing or using cybersecurity related technologies
- Management practices
- Monitoring, testing and evaluating cybersecurity controls' effectiveness
- Multidiscipline aspect of cybersecurity
- Offensive and defensive security practices
- Operating systems security

- Penetration testing procedures
- Penetration testing standards, methodologies and frameworks
- Privacy impact assessment standards, methodologies and frameworks
- Privacy-Enhancing Technologies (PET)
- Resource management
- Responsible information disclosure procedures
- Risk management recommendations and best practices
- Risk management standards, methodologies and frameworks
- Risk management tools
- Security architecture reference models
- Threat actors Tactics, Techniques and Procedures (TTPs)

Courses

Business Resilience and Incident Management

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Use and apply CTI platforms and tools • Apply auditing tools and techniques • Build resilience against points of failure across the architecture • Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks • Practice all technical, functional and operational aspects of cybersecurity incident handling and response • Identify threat actors TTPs and campaigns • Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls • Analyse and consolidate organisation’s quality and risk management practices • Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards • Anticipate required changes to the organisation’s information security strategy and formulate new plans 	<ul style="list-style-type: none"> • Threat actors Tactics, Techniques and Procedures (TTPs) • Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks • Digital forensics analysis procedures • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Incident handling tools • Cybersecurity controls and solutions • Incident handling communication procedures • Computer Security Incident Response Teams (CSIRTs) operation • Cybersecurity procedures • Cybersecurity risks • Risk management recommendations and best practices • Cross-domain and border-domain knowledge related to cybersecurity • Incident handling recommendations and best practices • Incident handling standards, methodologies and frameworks

Cloud Architectures and Security

ECSF Skills	ECSF Knowledge
-------------	----------------

- Collaborate with other team members and colleagues
- Model threats, actors and TTPs
- Identify and solve cybersecurity-related issues
- Conduct technical analysis and reporting
- Select appropriate specifications, procedures and controls
- Build resilience against points of failure across the architecture
- Implement cybersecurity recommendations and best practices
- Decompose and analyse systems to identify weaknesses and ineffective controls
- Identify threat actors TTPs and campaigns
- Work on operating systems, servers, clouds and relevant infrastructures
- Manage cybersecurity resources
- Coordinate the integration of security solutions
- Assess and enhance an organisation's cybersecurity posture
- Communicate, present and report to relevant stakeholders
- Develop and communicate, detailed and reasoned investigation reports
- Assess the security and performance of solutions
- Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles

- Offensive and defensive security practices
- Responsible information disclosure procedures
- Incident handling communication procedures
- Incident handling standards, methodologies and frameworks
- Incident handling recommendations and best practices
- Cybersecurity recommendations and best practices
- Security architecture reference models
- Cybersecurity controls and solutions
- Cyber threats
- Computer networks security
- Operating systems security
- Cybersecurity-related technologies
- Cyber threat actors
- Risk management recommendations and best practices

Communications & Cybersecurity

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Communicate, present and report to relevant stakeholders • Communicate, explain and adapt legal and regulatory requirements and business needs • Communicate, coordinate and cooperate with internal and external stakeholders 	<ul style="list-style-type: none"> • Management practices • Incident handling communication procedures

Cybercrime and Cybersecurity

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Work under pressure • Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks • Communicate, explain and adapt legal and regulatory requirements and business needs • Explain and present digital evidence in a simple, straightforward and easy to understand way • Analyse and comply with cybersecurity-related laws, regulations and legislations • Conduct ethical hacking 	<ul style="list-style-type: none"> • Multidiscipline aspect of cybersecurity • Privacy impact assessment standards, methodologies and frameworks • Legal, regulatory and legislative requirements on releasing or using cybersecurity related technologies • Cybersecurity-related certifications • Conformity assessment standards, methodologies and frameworks • Criminal investigation procedures, standards, methodologies and frameworks • Cybersecurity related laws, regulations and legislations • Legal, regulatory and legislative compliance requirements, recommendations and best practices

Cybersecurity Battleground: Threats, Vulnerabilities and Technologies

--	--

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Analyse and consolidate organisation's quality and risk management practices • Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy • Assess and enhance an organisation's cybersecurity posture • Communicate, present and report to relevant stakeholders • Develop, champion and lead the execution of a cybersecurity 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 • Monitor new advancements in cybersecurity-related technologies • Provide training towards cybersecurity and data protection professional certifications • Understand, practice and adhere to ethical requirements and standards • Utilise existing cybersecurity-related training resources • Identify non-cyber events with implications on cyber-related activities • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing 	<ul style="list-style-type: none"> • Incident handling communication procedures • Incident handling recommendations and best practices • Incident handling standards, methodologies and frameworks • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Legacy cybersecurity procedures • Threat actors Tactics, Techniques and Procedures (TTPs) • Auditing standards, methodologies and frameworks • Risk management recommendations and best practices • Risk management standards, methodologies and frameworks • Risk management tools • Digital forensics recommendations and best practices • Penetration testing procedures • Penetration testing standards, methodologies and frameworks

Foundations of Cryptography

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Analyse and comply with cybersecurity-related laws, regulations and legislations • Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles • Conduct technical analysis and reporting • Monitor new advancements in cybersecurity-related technologies • Think creatively and outside the box 	<ul style="list-style-type: none"> • Computer networks security • Operating systems security • Computer systems vulnerabilities • Cybersecurity recommendations and best practices • Privacy-Enhancing Technologies (PET)

Fundamental Principles and Risk Management of Cybersecurity

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Conduct ethical hacking • 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 	<ul style="list-style-type: none"> • Cybersecurity maturity models • Cybersecurity risks

Information Security Governance

--	--

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Analyse and comply with cybersecurity-related laws, regulations and legislations • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Collect, analyse and correlate cyber threat information originating from multiple sources • Select appropriate specifications, procedures and controls • Communicate, present and report to relevant stakeholders • Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards 	<ul style="list-style-type: none"> • Incident handling standards, methodologies and frameworks • Incident handling recommendations and best practices • Incident handling communication procedures • Conformity assessment standards, methodologies and frameworks

Information Security Leadership (the CISO Fundamentals)

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Anticipate required changes to the organisation's information security strategy and formulate new plans • Assess and enhance an organisation's cybersecurity posture • Collaborate with other team members and colleagues • Communicate, coordinate and cooperate with internal and external stakeholders • Communicate, present and report to relevant stakeholders • Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements • Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools • Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles • Develop, champion and lead the execution of a cybersecurity strategy • Analyse and consolidate organisation's quality and risk management practices • Establish a cybersecurity plan • Explain and communicate data protection and privacy topics to stakeholders and users • Follow and practice auditing frameworks, standards and methodologies • Identify and select appropriate pedagogical approaches for the intended audience • Identify and solve cybersecurity-related issues • Influence an organisation's cybersecurity culture • Manage cybersecurity resources • Motivate and encourage people • Review and enhance security documents, reports, SLAs and ensure the security objectives • Utilise existing cybersecurity-related training resources 	<ul style="list-style-type: none"> • Risk management tools • Auditing standards, methodologies and frameworks • Risk management standards, methodologies and frameworks • Risk management recommendations and best practices

Information Security Management

ECSF Skills	ECSF Knowledge
-------------	----------------

- Analyse and consolidate organisation's quality and risk management practices
- Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls
- Coordinate the integration of security solutions
- Manage cybersecurity resources
- Integrate cybersecurity solutions to the organisation's infrastructure
- Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards

- Management practices
- Risk management recommendations and best practices
- Risk management standards, methodologies and frameworks
- Risk management tools

Information System Security

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls • Anticipate cybersecurity threats, needs and upcoming challenges • Assess the security and performance of solutions 	<ul style="list-style-type: none"> • Cybersecurity attack procedures • Cybersecurity recommendations and best practices • Cybersecurity controls and solutions • Computer systems vulnerabilities

Management of IT Projects

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Manage cybersecurity resources 	<ul style="list-style-type: none"> • Resource management • Management practices

Practice in Company

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy • Identify and solve cybersecurity-related issues • Assess and enhance an organisation's cybersecurity posture 	<ul style="list-style-type: none"> • Cybersecurity recommendations and best practices • Cybersecurity-related technologies • Cybersecurity-related research, development and innovation (RDI)

Security Architecture

ECSF Skills	ECSF Knowledge
-------------	----------------

- Assess the security and performance of solutions
- Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks
- Build resilience against points of failure across the architecture
- Decompose and analyse systems to develop security and privacy requirements and identify effective solutions
- Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards

Security Architecture Securing the Landscape

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Build a cybersecurity risk-aware environment • Build resilience against points of failure across the architecture • Collect, analyse and correlate cyber threat information originating from multiple sources • Decompose and analyse systems to develop security and privacy requirements and identify effective solutions • Decompose and analyse systems to identify weaknesses and ineffective controls • Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles • Draw cybersecurity architectural and functional specifications • Guide and communicate with implementers and IT/OT personnel • Identify and solve cybersecurity-related issues • Integrate cybersecurity solutions to the organisation's infrastructure • Automate threat intelligence management procedures • Propose cybersecurity architectures based on stakeholder's needs and budget • Generate new ideas and transfer theory into practice • Conduct technical analysis and reporting • Assess the security and performance of solutions 	<ul style="list-style-type: none"> • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Legal, regulatory and legislative requirements on releasing or using cybersecurity related technologies • Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks • Cyber threats • Cyber threat actors • Risk management recommendations and best practices • Risk management standards, methodologies and frameworks • Risk management tools • Digital forensics analysis procedures • Digital forensics recommendations and best practices

Security Controls Governance, Risk, Compliance and Certification

ECSF Skills	ECSF Knowledge
	<ul style="list-style-type: none"> • Conformity assessment standards, methodologies and frameworks • Cybersecurity controls and solutions • Cybersecurity policies • Cybersecurity standards, methodologies and frameworks • Cybersecurity-related requirements analysis • Monitoring, testing and evaluating cybersecurity controls' effectiveness

- Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks
- Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls
- Assess and enhance an organisation's cybersecurity posture
- Build a cybersecurity risk-aware environment
- Follow and practice auditing frameworks, standards and methodologies
- Identify and solve cybersecurity-related issues
- Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards
- Integrate cybersecurity solutions to the organisation's infrastructure
- Propose and manage risk-sharing options
- Select appropriate specifications, procedures and controls
- Analyse and consolidate organisation's quality and risk management practices

Security Fundamentals

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Collect, analyse and correlate cyber threat information originating from multiple sources • Anticipate cybersecurity threats, needs and upcoming challenges • Follow and practice auditing frameworks, standards and methodologies • Define and apply maturity models for cybersecurity management 	<ul style="list-style-type: none"> • Cybersecurity risks • Cybersecurity policies • Cybersecurity procedures • Cybersecurity related laws, regulations and legislations • Risk management standards, methodologies and frameworks • Cyber threats • Computer systems vulnerabilities • Computer networks security • Cybersecurity standards, methodologies and frameworks • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Cyber threat actors • Cybersecurity trends

Security Management and Law

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none"> • Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies • 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 • Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks • Analyse and comply with cybersecurity-related laws, regulations and legislations 	<ul style="list-style-type: none"> • Cybersecurity related laws, regulations and legislations • Cybersecurity policies • Cybersecurity standards, methodologies and frameworks • Ethical cybersecurity organisation requirements

Technology Risk Governance

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none">• Select appropriate specifications, procedures and controls• Analyse and consolidate organisation's quality and risk management practices• Build a cybersecurity risk-aware environment• Monitor new advancements in cybersecurity-related technologies• Implement cybersecurity recommendations and best practices• Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards• Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks• Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks	<ul style="list-style-type: none">• Cybersecurity policies• Digital forensics standards, methodologies and frameworks• Risk management tools• Risk management standards, methodologies and frameworks• Cybersecurity risks• Incident handling recommendations and best practices• Legal, regulatory and legislative requirements on releasing or using cybersecurity related technologies• Management practices

The challenges for Information Security

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none">• Coordinate the integration of security solutions• Assess and enhance an organisation's cybersecurity posture• Monitor new advancements in cybersecurity-related technologies• Work on operating systems, servers, clouds and relevant infrastructures	<ul style="list-style-type: none">• Cybersecurity recommendations and best practices• Risk management standards, methodologies and frameworks• Cybersecurity-related technologies• Monitoring, testing and evaluating cybersecurity controls' effectiveness• Conformity assessment standards, methodologies and frameworks

Thesis

ECSF Skills	ECSF Knowledge
<ul style="list-style-type: none">• Analyse and comply with cybersecurity-related laws, regulations and legislations• Work ethically and independently; not influenced and biased by internal or external actors• Think creatively and outside the box	<ul style="list-style-type: none">• Cybersecurity recommendations and best practices• Multidiscipline aspect of cybersecurity• Cybersecurity trends• Cybersecurity-related technologies• Cybersecurity-related research, development and innovation (RDI)



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101123430.

Legal Disclaimer

The European Commission's support to produce this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

Copyright © 2023 by Digital4Security Consortium

Digital4Security Course Curriculum | [Brno University of Technology](#)



Digital4Security

Shaping Europe's cyber future

