Project No. 101083594 Project start: 2022-12-01
Call: DIGITAL-2021-SKILLS-01 Project duration: 39 months

CyberSecPro

D5.3
CyberSecPro Certification Schema

Document Identification	
Due date	2026-02-28
Submission date	2026-02-28
Version	1.0

Related WP	WP5	Dissemination Level	PU – Public
Lead Participant	UPRC	Lead Author	Dimitrios Kallergis, Nineta Polemi, Christos Douligeris (UPRC)
Contributing Participants	UPRC, TUC, APIRO, MAG, COFAC, TUBS, UNINOVA, FP, FCT	Related Deliverables	D2.1, D2.3, D3.1, D3.2, D3.3, D3.4, D3.5

Abstract: The CyberSecPro project identified the lack of a unified European certification framework for professional cybersecurity training, resulting in fragmented, non-interoperable programmes with limited mutual recognition. This issue is particularly acute in sector-specific contexts, where rapid digitalisation contrasts with low cybersecurity maturity and inconsistent skill development, restricting cross-sector mobility. The project proposes a structured certification schema comprising modular training aligned with defined competencies and subject to higher-level recognition, such as by the ECCC. The sector-specific professional training scheme integrates theoretical and practical learning, maps micro-credentials to ECTS credits, aligns with ECSF profiles and competences, and offers trainees up to 60 ECTS credits.

The deliverable reflects the Task 5.4 outcomes.

Co-funded by the
European Union

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

This document is issued within the CyberSecPro project. This project has received funding from the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594.

Executive Summary

The CyberSecPro project seeks to address a structural deficiency within the European Union, namely the absence of a harmonised certification scheme for professional cybersecurity training, and to propose a common European solution. At present, a broad range of cybersecurity training programmes is available across the EU; however, these programmes adopt heterogeneous methodologies and frameworks, resulting in certifications that are not interoperable or mutually recognisable. Furthermore, no European-level authority currently exists with a formal mandate to approve or validate such professional cybersecurity training programmes.

This challenge is further compounded in the context of **sector-specific cybersecurity training**. All economic sectors increasingly depend on digitalisation and the adoption of emerging technologies, including artificial intelligence. Despite this growing reliance, cybersecurity maturity levels across sectors remain comparatively low, creating a sustained need for continuous and targeted professional training. Existing sector-specific training programmes are highly fragmented, lack interoperability, and fail to ensure the consistent development of skills and capabilities. Consequently, professionals face limited mobility across sectoral environments, despite the transversal nature of many cybersecurity competencies.

To address these challenges, the CyberSecPro project proposes the establishment of a **cybersecurity professional training schema**. Such a schema is defined as a structured training programme, or a coherent set of modular learning components, designed to equip learners with sector-specific cybersecurity knowledge, skills, and competencies. A central requirement of the proposed scheme is formal recognition and approval by a competent higher-level authority, ensuring quality assurance, consistency, and trust across the European Union.

Upon successful completion of a full programme or designated modules aligned with the schema, participants would be awarded a **certification** issued or endorsed by the relevant higher authority. This certification would constitute formal recognition of the individual's demonstrated expertise and capabilities in cybersecurity within a sector-specific context. Such certifications are essential for professionals seeking to enter or progress within cybersecurity-related roles, as they provide employers and clients with assurance that the certified individual meets clearly defined standards of proficiency and competence.

Professional training schemes may differ in duration, scope, content, and delivery format, ranging from short courses targeting specific skill sets to comprehensive programmes covering broader knowledge domains. These schemes may be delivered by a variety of providers, including academic institutions, professional associations, industry bodies, and private training organisations.

The training scheme proposed under the CyberSecPro project emphasises an integrated approach that combines theoretical instruction with practical, hands-on training. This approach is intended to ensure that participants develop both a sound conceptual understanding and the practical competencies required to address real-world cybersecurity challenges.

This document consolidates the certification schemes proposed in the deliverable D3.2. The consolidated schema introduces mathematical formulas for mapping the assigned micro-credentials to ECTS credits for each CyberSecPro module which corresponds to a type of a cybersecurity sector-specific training course. Additionally, the proposed schema includes a concrete mapping to the ECSF framework's profiles and competences.

Document information

Contributors

Name	Beneficiary
Dimitrios Kallergis, Christos Douligeris, Nineta Polemi	UPRC
Pinelopi Kyranoudi, Sotiris Ioannidis, Markos Kimionis, Evripidis Sotiriadis	TUC
Iro Chatzopoulou	APIRO
Spiros Borotis	MAG
Daniel Silveira	COFAC
Antonios Ntib	TUBS
Paulo Figueiras, Ruben Costa, Vasco Delgado-Gomes	UNINOVA
Christos Grigoriadis	FP

Reviewers

Name	Beneficiary
Kitty Kioskli	Trustilio
Shareeful Islam	SLC
Jeldo Meppen	ACEEU (as QM)

History

Version	Date	Contributor(s)	Comment(s)
0.1	2025-02-07	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi	1st Draft of ToC
0.2	2025-03-07	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi	2nd Draft of ToC
0.3	2025-04-04	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi	3rd Draft of ToC

0.4	2025-04-17	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi, Daniel Silveira, Spiros Borotis	Contribution in chapters 1 and 2
0.5	2025-05-28	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi, Daniel Silveira, Spiros Borotis, Pinelopi Kyranoudi, Sotiris Ioannidis, Markos Kimionis, Evripidis Sotiriadis	Contribution in chapter 2
0.6	2025-07-22	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi, Daniel Silveira, Spiros Borotis	Contribution in chapters 2 and 3
0.7	2025-09-17	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi, Daniel Silveira, Spiros Borotis, Pinelopi Kyranoudi, Sotiris Ioannidis, Markos Kimionis, Evripidis Sotiriadis, Antonios Ntib, Christos Grigoriadis, Paulo Figueiras, Ruben Costa, Vasco Delgado-Gomes	Contribution in chapters 1, 2, 3, and 4
0.71	2025-10-01	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi, Daniel Silveira, Spiros Borotis, Iro Chatzopoulou	Contribution in chapter 3
0.72	2025-12-01	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi, Daniel Silveira, Spiros Borotis, Pinelopi Kyranoudi, Sotiris Ioannidis, Markos Kimionis, Evripidis Sotiriadis, Iro Chatzopoulou, Christos Grigoriadis, Paulo Figueiras, Ruben Costa, Vasco Delgado-Gomes	Contribution in chapters 2 and 4
0.73	2025-12-29	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi, Daniel Silveira, Pinelopi Kyranoudi, Sotiris Ioannidis, Markos Kimionis, Evripidis Sotiriadis, Iro Chatzopoulou	Contribution in chapters 1, 2, 3 and 4
0.74	2026-01-02	Dimitrios Kallergis, Christos Douligeris, Nineta Polemi, Daniel Silveira, Spiros Borotis, Pinelopi Kyranoudi, Sotiris Ioannidis, Markos Kimionis,	Contribution in chapters 3 and 4

		Evripidis Sotiriadis, Iro Chatzopoulou	
0.75	2026-01-04	Daniel Silveira, Christos Douligeris	High level review
0.76	2026-01-23	Kitty Kioskli, Shareeful Islam	1st review
0.77	2026-02-02	Dimitrios Kallergis	Contribution in all chapters
0.78	2026-02-09	Shareeful Islam, Kitty Kioskli	2nd review
0.79	2026-02-16	Dimitrios Kallergis	Contribution in chapter 4
0.80	2026-02-25	Daniel Silveira, Christos Douligeris, Jeldo Meppen	High-level review
0.81	2026-02-25	Atiyeh Sadeghi	Layout and editorial improvement
0.82	2026-02-27	Dimitrios Kallergis	Layout improvement and minor corrections
1.0	2026-02-28	Atiyeh Sadeghi	Final check, preparation and submission process

Table of Contents

List of Figures

List of Tables

1 Introduction

Within the CyberSecPro project, a key structural gap was identified, namely the absence of a unified certification framework for professional cybersecurity training. As a consequence, the wide range of existing cybersecurity training programmes adopts heterogeneous approaches, resulting in certifications that lack interoperability and mutual recognition. Moreover, there is currently no designated European-level authority responsible for the formal approval or endorsement of such professional training programmes.

This fragmentation is further exacerbated in the context of **sector-specific professional training**. Across all economic sectors—including, but not limited to, transport, energy, and healthcare—accelerated digitalisation has led to the extensive adoption of information and communication technologies and emerging technologies such as artificial intelligence. Despite this increasing technological dependency, cybersecurity maturity levels in many sectors remain relatively low, creating a sustained need for continuous and targeted professional training. Existing sector-specific cybersecurity programmes are largely fragmented, lack interoperability, and fail to deliver harmonised skill sets and capabilities. As a result, employees face limited professional mobility across sectoral environments, despite the transversal nature of cybersecurity competencies.

For the purposes of this work, a **certification schema** is understood as a structured and coherent training programme, or set of modular learning components, designed to equip learners with defined knowledge, skills, and competencies in cybersecurity tailored to specific sectoral contexts. Such schemes should be subject to recognition or approval by a competent higher-level authority, such as the European Cybersecurity Competence Centre (ECCC), in order to ensure consistency, quality, and trust.

Upon successful completion of a professional training scheme or its constituent modules, participants are awarded a **certification** issued or endorsed by a higher authority. This certification constitutes formal recognition of the individual's acquired competencies and professional capabilities. In sectoral cybersecurity contexts, such certifications play a critical role in supporting career entry and progression, as they provide employers and clients with assurance that certified individuals meet established standards of proficiency and competence relevant to the cybersecurity requirements of the respective sector.

The professional training schema proposed within the CyberSecPro project adopts an integrated approach, combining theoretical instruction with practical, hands-on training, thereby supporting both conceptual understanding and applied competence development.

The deliverable D5.3 consolidates and finalises the certification schemes proposed in the deliverable D3.2. The consolidated schema introduces mathematical formulas for mapping the assigned micro-credentials to ECTS credits for each CyberSecPro module which corresponds to a type of a cybersecurity sector-specific training course. Additionally, the proposed schema includes a concrete mapping to the ECSF framework's profiles and competences, and it offers 60 ECTS credits to the trainees.

This document represents the closure of the certification schema work within WP5.

1.1 Background

The necessity for specialized industry-driven training has been highlighted in deliverables D2.1 and D2.3, which pointed out the need for further training across 10 Key Areas (KA). Based on this critical analysis, the CSP project, in D2.3, has proposed the development of 12 modules specifically designed to address these needs, while deliverable D3.1 outlines CSP programme's has focused on training modules and model syllabi, templates, and key elements for these individual modules. The D3.2,

addressed the gap for common industry-driven cybersecurity professional training programmes and proposed three training schemes to tackle with this issue.

This deliverable consolidates and finalises the certification schemes proposed in D3.2, while it maps micro-credentials to ECTS credits, it aligns with ECSF profiles and competences, and it offers trainees up to 60 ECTS credits in a concrete scheme.

1.2 Relation to Other Work Packages and Deliverables

This deliverable capitalises the knowledge gained in deliverables D2.1, D2.3, and D3.1, and mostly D3.2, it complements and extends the work done in these CyberSecPro Tasks and it proposes an industry-driven cybersecurity certification schema.

1.3 Methodology

In the context of D5.3, we present the adopted methodology under the scope of updating the addressed gaps for common industry-driven cybersecurity professional training programmes and proposing schemes that fulfil this need. Any updates are given in comparison to the deliverable D3.2.

Phase 1: We thoroughly assess the various EU and international bodies in terms of their certification efforts on the professional trainings that especially focus on sector-specific cybersecurity. At this step, we also illustrate EU initiatives that aim to harmonise the cybersecurity certification landscape.

Phase 2: We include common elements, considerations of certification bodies. This information is combined with different scales and measurements that are currently used.

Phase 3: We present the key factors and standards that feed the consolidated CyberSecPro certification scheme.

2 Certification Landscape Related to Cybersecurity Training

The deliverables D2.1 and D2.2 review the EU and international efforts in cybersecurity professional and academic trainings as well as the bodies which are involved in these trainings, while the deliverable D3.2 assesses the various bodies in terms of the trainings certification efforts and especially for sector-specific cybersecurity trainings.

In this chapter, we ***(a)*** provide information on how several EU and international cybersecurity certification bodies map their credentials to the European Cybersecurity Skills Framework (ECSF), and offer any updates regarding their training offerings in the cybersecurity trainings certification landscape, ***(b)*** examine several National Cybersecurity Strategies (NCSS) and focus on the extent to which training-related certification is reflected in strategic objectives, selected policy instruments, and governance arrangements, ***(c)*** shed light on multiple EU initiatives which cope with the challenge of cybersecurity trainings and their certification issuing process.

This chapter mainly updates the findings of the corresponding chapter 2 of the deliverable D3.2 and it serves as input and evidence for the consolidation of the CyberSecPro certification schema.

2.1 International Certification Bodies

During the past two years, leading certification bodies have mapped their credentials to the European Cybersecurity Skills Framework (ECSF). The mappings are hosted within the bodies' websites as well as in the ENISA ECSF[1] webspace.

Currently, the mappings provided are from the following certification bodies: CompTIA, ISACA, ISC2, SANS / GIAC, CREST, EC-Council, Fortinet and Hachthebox.

2.1.1 CompTIA

Figure 1 is provided by CompTIA[2] and it illustrates an information pathway for identifying the knowledge and skills alignment between CompTIA certifications and the roles as defined in ENISA's European Cybersecurity Skills Framework (ECSF).

[1] https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf/certifications-mapped-to-the-ecsf
[2] https://lecbyo.files.cmp.optimizely.com/download/451be51c2a9511f0a2b97252cf4a59ca

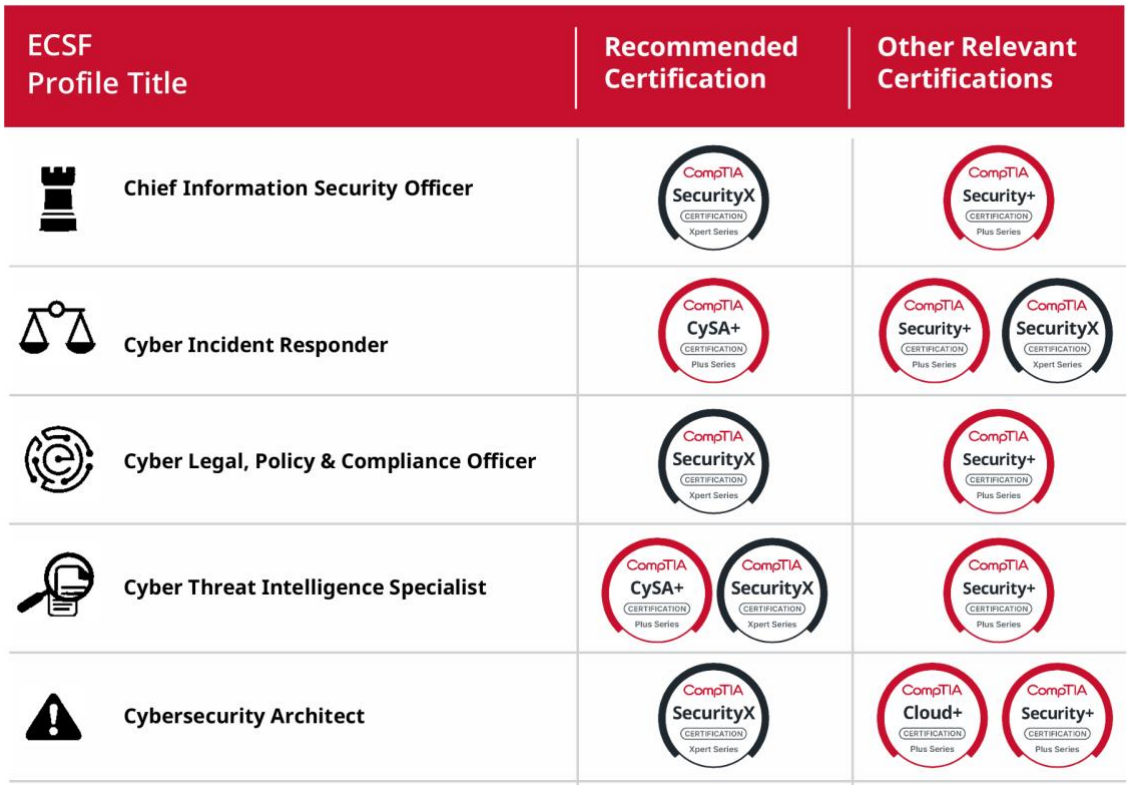

Figure 1. CompTIA Certification Coverage of ECSF Roles

2.1.2 ISACA

Figures 2, 3, and 4 are provided by ISACA[3] and they illustrate a pathway for identifying the knowledge and skills alignment between ISACA credentials and the roles as defined in ENISA's European Cybersecurity Skills Framework (ECSF). The credentials referenced in the following Figures can be combined with ISACA certifications to provide vertical expertise in any of the professional titles on AI, Blockchain, Cloud and IoT.

[3] https://www.isaca.org/career-center/european-cybersecurity-skills-framework-and-isaca-credentials

ECSF Profile	ISACA Cert	Notes
Chief Information Security Officer (CISO)	CISM Certified Information Security Manager. An ISACA® Certification Certified Information Security Manager (CISM)	CISM indicates expertise in information security governance, program development and management, incident management and risk management.
Cyber Incident Responder	CCOA Certified Cybersecurity Operations Analyst. An ISACA® Certification Certified Cybersecurity Operations Analyst (CCOA)	CCOA empowers cybersecurity professionals to prove their hands-on abilities in effectively analyzing, detecting and responding to cyber threats.
Cyber Legal, Policy & Compliance Officer	CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification Certified Data Privacy Solutions Engineer (CDPSE).	CDPSE focuses on validating the technical skills and knowledge it takes to assess, build, and implement a comprehensive privacy solution.
	and/or	
	CISM Certified Information Security Manager. An ISACA® Certification Certified Information Security Manager (CISM)	CISM indicates expertise in information security governance, program development and management, incident management and risk management.
Cyber Threat Intelligence Specialist	CRISC Certified in Risk and Information Systems Control. An ISACA® Certification Certified in Information System Risk and Control (CRISC)	CRISC validates your experience in building a well-defined, agile risk-management program, based on best practices to identify, analyze, evaluate, assess, prioritize, and respond to risks. This enhances benefits realization and delivers optimal value to stakeholders.
	and/or	
	IT RISK FUNDAMENTALS An ISACA® Certificate IT Risk Fundamentals Certificate	IT Risk Fundamentals Certificate and related training is ideal for professionals who wish to learn about risk and information and technology (I&T)-related risk, who currently interact with risk professionals, or are new to risk and interested in working as a risk or IT Risk professional.

Figure 2. ISACA credentials for assisting cybersecurity career paths in Europe (part I)

Cyber Threat Intelligence Specialist	Certified in Risk and Information Systems Control. An ISACA® Certification Certified in Information System Risk and Control (CRISC)	CRISC validates your experience in building a well-defined, agile risk-management program, based on best practices to identify, analyze, evaluate, assess, prioritize, and respond to risks. This enhances benefits realization and delivers optimal value to stakeholders.
	and/or	
	IT RISK FUNDAMENTALS An ISACA® Certificate IT Risk Fundamentals Certificate	IT Risk Fundamentals Certificate and related training is ideal for professionals who wish to learn about risk and information and technology (I&T)-related risk, who currently interact with risk professionals, or are new to risk and interested in working as a risk or IT Risk professional.
Cybersecurity Architect	Information Technology Certified Associate. An ISACA® Certification Information Technology Certified Associate (ITCA)	If you are a student or new to the profession, build your IT working knowledge and skills with the ITCA certificate and become a cybersecurity architect.
	and/or	
	CYBERSECURITY FUNDAMENTALS An ISACA® Certificate Cybersecurity Fundamentals Certificate	Cybersecurity Fundamentals include threat landscape, securing assets, information security fundamentals, and security operations and response.
	and	
	Certified Data Privacy Solutions Engineer. An ISACA® Certification Certified Data Privacy Solutions Engineer (CDPSE).	CDPSE focuses on validating the technical skills and knowledge it takes to assess, build, and implement a comprehensive privacy solution.
Cybersecurity Auditor	Certified Information Systems Auditor. An ISACA® Certification Certified Information Systems Auditor (CISA)	CISA is world-renowned as the standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems.
	and/or	
	CYBERSECURITY AUDIT An ISACA® Certificate Cybersecurity Audit Certificate	ISACA's Cybersecurity Audit Certificate Program provides audit/assurance professionals with the knowledge needed to excel in cybersecurity audits, and IT risk professionals with an understanding of cyber-related risk and mitigating controls.

Figure 3. ISACA credentials for assisting cybersecurity career paths in Europe (part II)

Cybersecurity Educator	CYBERSECURITY FUNDAMENTALS An ISACA® Certificate Cybersecurity Fundamentals Certificate	Cybersecurity Fundamentals include threat landscape, securing assets, information security fundamentals, and security operations and response.
	and/or (for more in-depth expertise)	
	CISM Certified Information Security Manager. An ISACA® Certification Certified Information Security Manager (CISM)	CISM indicates expertise in information security governance, program development and management, incident management and risk management.
Cybersecurity Implementor	CYBERSECURITY FUNDAMENTALS An ISACA® Certificate Cybersecurity Fundamentals Certificate	Cybersecurity Fundamentals include threat landscape, securing assets, information security fundamentals, and security operations and response.
	and/or	
	CISM Certified Information Security Manager. An ISACA® Certification Certified Information Security Manager (CISM)	CISM indicates expertise in information security governance, program development and management, incident management and risk management.
Cybersecurity Researcher	CISM Certified Information Security Manager. An ISACA® Certification Certified Information Security Manager (CISM)	CISM indicates expertise in information security governance, program development and management, incident management and risk management.
Cybersecurity Risk Manager	CRISC Certified in Risk and Information Systems Control. An ISACA® Certification Certified in Information System Risk and Control (CRISC)	CRISC validates your experience in building a well-defined, agile risk-management program, based on best practices to identify, analyze, evaluate, assess, prioritize and respond to risks. This enhances benefits realization and delivers optimal value to stakeholders.

Figure 4. ISACA credentials for assisting cybersecurity career paths in Europe (part III)

2.1.3 ISC2

Figure 5 is provided by ISC2[4] and it recommends the learners the ISC2 certifications which will help them acquire the knowledge and skills required for roles under ENISA's European Cybersecurity Skills Framework (ECSF). The recommendations are based on the coverage of knowledge and skills topics

[4] https://www.isc2.org/training/isc2-certification-coverage-of-ecsf-roles

for each role, rather than coverage of tasks, and limited to roles where ISC2 certifications provide a high level of coverage.

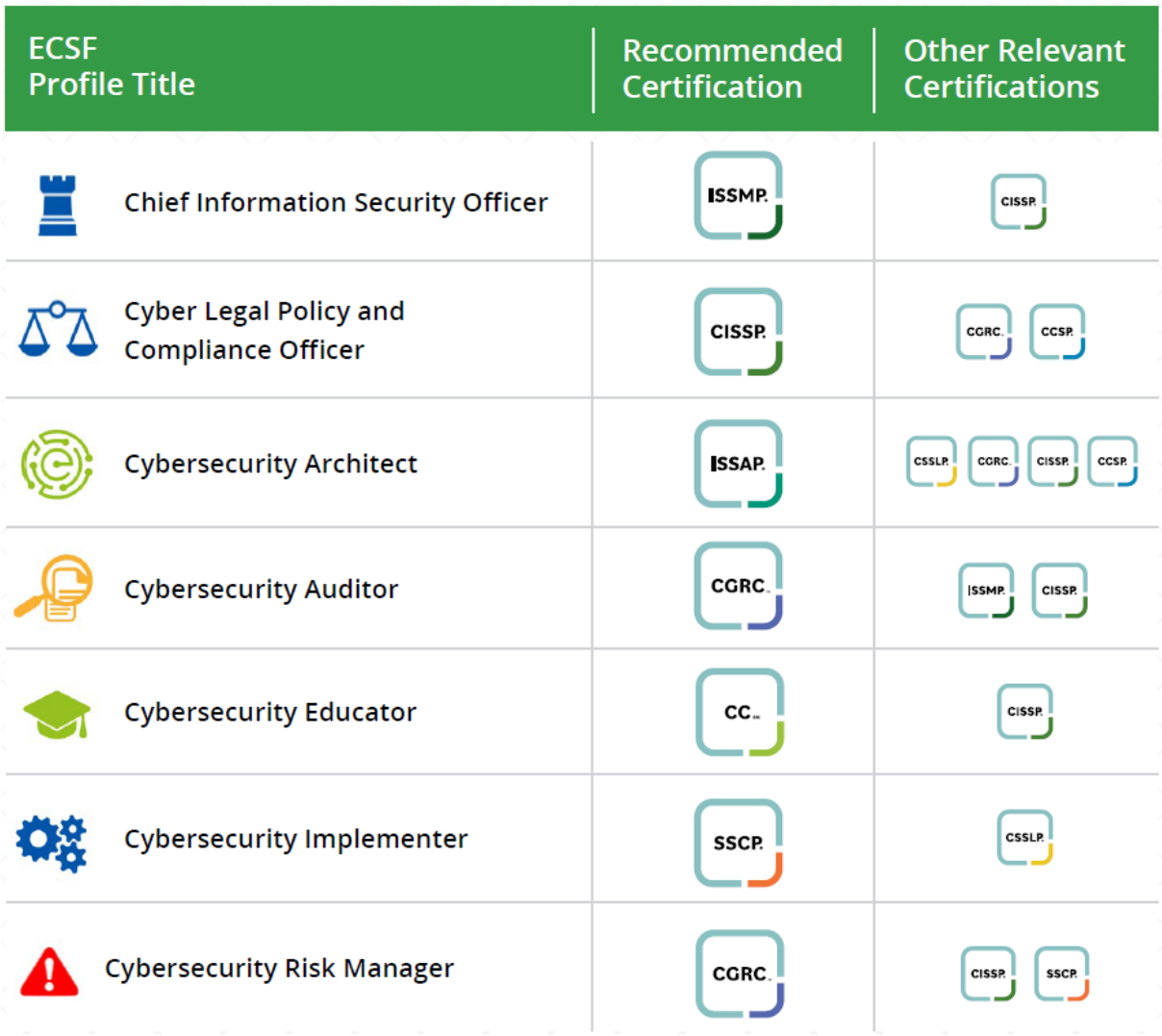

Figure 5. ISC2 certifications to acquire the knowledge and skills required for roles under ECSF

2.1.4 SANS / Global Information Assurance Certifications (GIAC)

SANS and Global Information Assurance Certifications (GIAC)[5] also provide concrete learning paths aligned to the European Cybersecurity Skills Framework (ECSF). Any cybersecurity-related role is summarised in each of the 12 ECSF profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies, and interdependencies. These learning paths provide a common understanding of the relevant roles, competencies, skills and knowledge required, they facilitate recognition of cybersecurity skills, and support the design of cybersecurity-related training programmes.

[5] https://www.sans.org/job-roles/cyber-incident-responder

2.1.5 CREST

CREST[6] also maps its certifications to the ECSF framework to better support individuals in their career progression, and enable organisations and training providers to provide improved services for clients and training for their employees. In detail, CREST offers certifications in 3 curriculum areas: *Penetration Testing*, *Threat Intelligence*, and *Incident Response* and at three levels Practitioner (Introductory), Registered (Intermediate) and Certified (Advanced). The more advanced the exam then the more technical detail will be assessed which will determine the capability and expertise of the candidate.

2.1.6 EC-Council

In alignment with the European Cybersecurity Skills Framework (ECSF), EC-Council[7] offers targeted certifications and training programs that empower professionals with essential skills and knowledge required for the most in-demand cybersecurity roles across Europe. By mapping their certifications to the ECSF, the EC-Council provides a clear pathway for individuals and organizations to understand how our certifications prepare professionals for roles within the ECSF framework.

Figure 6 presents these mappings.

Job Profile Titles	EC-Council Programs
Chief Information Security Officer (CISO)	C|CISO Certified Chief Information Security Officer (C|CISO)
Cyber Incident Responder	E|CIH EC-Council Certified Incident Handler (E|CIH)
Cyber Legal, Policy & Compliance Officer	C|CISO Certified Chief Information Security Officer (C|CISO)
Cyber Threat Intelligence Specialist	C|TIA Certified Threat Intelligence Analyst (C|TIA)
Cybersecurity Implementer	C|ND Certified Network Defender (C|ND)
Digital Forensics Investigator	C|HFI Computer Hacking Forensic Investigator (C|HFI)
Penetration Tester	C|PENT Certified Penetration Testing Professional (C|PENT)

Figure 6. EC-Council mappings to ECSF roles

[6] https://www.crest-approved.org/skills-certifications-careers/european-cybersecurity-skills-framework/
[7] https://www.eccouncil.org/european-cybersecurity-skills-framework-ecsf-ec-council/

2.1.7 Fortinet

As referred to their website, the purpose of mapping the Fortinet[8] courses to the European Cybersecurity Skills Framework (ECSF) is to create a career path, allowing individuals to navigate their educational journey from curriculum to careers.

Figure 7 gathers this mapping information which categorises the certificated individuals as *associates*, *professionals*, *solution specialists*, and *experts* according to the level of expertise. The *Strong* notation refers to '*Strongly recommended = clear role fit (covers most tasks/skills)*', the *Support* notation refers to '*Also supports = partial overlap (tooling/knowledge helps the role)*', as the hyphen notation refers to '*Minimal = minimal alignment and overlap with specific skills, tasks, and knowledge related to the role*'.

NSE Levels	Associate	Professional				Solution Specialist				Expert
NSE Certification										
Chief Information Security Officer	-	Support	Support	Support	Support	Support	Support	Support	Support	Support
Cyber Incident Responder	Support	Support	**Strong**	Support	**Strong**	**Strong**	**Strong**	**Strong**	**Strong**	**Strong**
Cyber Legal, Policy and Compliance Officer	-	Support	Support	Support	Support	Support	Support	Support	Support	Support
Cyber Threat Intelligence Specialist	-	-	Support	-	Support	Support	**Strong**	-	Support	Support
Cybersecurity Architect	Support	Support	Support	Support	Support	**Strong**	**Strong**	**Strong**	**Strong**	**Strong**
Cybersecurity Auditor	-	Support	Support	Support	Support	Support	Support	Support	Support	Support
Cybersecurity Implementer	**Strong**	**Strong**	**Strong**	**Strong**	**Strong**	**Strong**	**Strong**	**Strong**	**Strong**	**Strong**
Cybersecurity Risk Manager	-	Support	Support	Support	Support	Support	Support	Support	Support	Support
Digital Forensics Investigator	-	Support	Support	-	-	Support	Support	-	-	Support

Figure 7. Fortinet's mappings against the ECSF roles

2.1.8 Hackthebox

Hack The Box (HTB)[9] has mapped its certification portfolio to ENISA's ECSF to support organizations and professionals in demonstrating competence against an EU-recognized standard. By mapping our highly hands-on, real-world certifications to ECSF role profiles, Hack the Box enables employers, partners, and learners to connect HTB qualifications directly to specific cybersecurity roles, workforce requirements, and regulatory or strategic initiatives across the EU.

HTB certifications map to ECSF role profiles, offering a clear pathway from entry-level to advanced expertise, while maintaining our signature focus on practical, lab-based training and operator-level realism. In detail, they notate as *(a)* '*Strongly aligned (Aligned Certifications/Certificate Programs)*' where certifications or certificate programs exist with direct and substantial coverage of the ECSF tasks, skills, and knowledge associated with a given profile, and as *(b)* '*Partially aligned (Relevant Certifications)*' where certifications exist that provide meaningful but supporting coverage of the ECSF profile. These credentials strengthen adjacent skills, extend a professional's scope, or support career progression into or around that role.

[8] https://www.fortinet.com/content/dam/fortinet/assets/reports/ftnt-nse-the-european-cybersecurity-skills-framework.pdf
[9] https://academy.hackthebox.com/european-cybersecurity-skills-framework

2.1.9 Discussion on the Certification Bodies Mappings to the ECSF Framework

Regarding the certification bodies' mappings to the ECSF framework, we identify the following characteristics:

1. In every case, there is a connection (mapping) between the certifications / certificates / training courses and the ECSF roles.
2. In most of the cases, there is no explanation or structured methodology regarding this mapping. The only exception identified was CREST which notes the following: "*the recommendations are based on the coverage of knowledge and skills topics for each role, rather than coverage of tasks', and are limited to roles where CREST certifications provide a high level of coverage. Cyber roles and capabilities often overlap and the ECSF is no different. The mapping of ECSF roles to CREST certifications considers a multi-skilled approach and offers alignment to additional roles and skills which may benefit organisations and individuals as they plan their capability development. Mapping methodology: CREST offers certifications in 3 curriculum areas. Penetration Testing, Threat Intelligence, and Incident Response and at three levels Practitioner (Introductory), Registered (Intermediate) and Certified (Advanced). The more advanced the exam then the more technical detail will be assessed which will determine the capability and expertise of the candidate'*.
3. Irrespectively of the mapping methodology used, the result is a connection between the Certificate and the ECSF role.
   Example: Regarding the role of the *Chief Information Security Officer (CISO)*, the first role profile of the ECSF, the following certifications are mapped:

Certification Body	Certification Issued
CompTIA:	CompTIA Security X
ISACA:	Certified Information Security Manager (CISM)
ISC2:	Information Systems Security Management Professional (ISSMP)
EC-Council:	Certified Chief Information Security Officer (CCISO)
Fortinet:	no clear role fit (covers most tasks/skills)
Hackthebox:	no aligned Certifications/Certificate Programs

4. When contrasting and comparing the certifications with the ECSF, minimum of no comparable information exists.
   Example: The publicly available information for ISACA Certified Information Security Manager (CISM) and for ISC2 Information Systems Security Management Professional (ISSMP). Table 2 gathers that information.

Table 1. Comparable information regarding the ISACA CISM and the ISC2 ISSMP certifications

	ISACA CISM	ISC2 ISSMP
Prerequisites	+ 2 Years or 7 years cumulative	-
Length of exam	4 hours	3 hours
No. of items	150	125
Item format	Multiple choice	Multiple choice
Passing grade	450 out of 800 points	700 out of 1000 points

Domains / Average Weight	1. Information Security Governance / 17%	1. Leadership and Organizational Management / 21%
	2. Information Security Risk Management / 20%	2. Systems Lifecycle Management / 15%
	3. Information Security Program / 33%	3. Risk Management / 20%
	4. Incident Management / 30%	4. Security Operations / 18%
	-	5. Contingency Management / 12%
	-	6. Law, Ethics, and Security Compliance Management / 14%
Notes	Five (5) or more years of experience in information security management. Experience waivers are available for a maximum of two (2) years	-

However, the comparison regarding the certified domain(s) gives more specific results. Table 2 gathers that results.

Table 2. Comparison between the domains covered by CISM and ISSMP

CISM Domain	**ISSMP Domain(s)**	**Coverage Level**	**Explanation**
Information Security Governance	Domain 1 – Leadership and Operational Management Domain 6 – Law, Ethics & Compliance	**High**	Both focus on security vision, governance, policy frameworks, leadership engagement, legal and regulatory alignment.
Information Security Risk Management	Domain 3 – Risk Management	**Very High**	Near one-to-one mapping: risk identification, assessment, treatment, monitoring, reporting.
Information Security Program	Domain 1 – Leadership & Operational Management Domain 2 – Systems Lifecycle Management	**High**	ISSMP adds deeper technical lifecycle and architecture elements; CISM remains more managerial.
Incident Management	Domain 4 – Security Operations Domain 5 – Contingency Management	**Very High**	Strong alignment across incident response, SOC, BCP/DRP, crisis management, and post-incident reviews.

In addition to the above checks, we provide a comparison between the Tasks of the *ECSF Chief Information Security Officer (CISO)* versus these Tasks coverage of *CISM* and *ISSMP*.

Table 3. Comparison between the tasks covered by ECSF CISO, ISACA CISM, and ISC2 ISSMP

ECSF CISO Main Tasks	CISM Coverage	ISSMP Coverage
Define cybersecurity vision, strategy & policies	Strong	Strong
Align cybersecurity with business strategy	Strong	Strong
Educate senior management on cyber risk	Strong	Strong
Ensure organisational cyber resilience	Strong	Strong
Approve & manage cyber risks	Strong	Very strong
Budget negotiation & resource allocation	Strong	Strong
Supervise ISMS	Strong	Strong
Monitor cybersecurity evolution & threats	Moderate	Strong
Manage incident reporting to leadership	Strong	Strong
Coordinate with authorities & communities	Moderate	Strong
Continuous capacity building	Moderate	Strong
Oversee operational security execution	Moderate	Very strong

A useful remark here is that any of the mentioned results is given by reviewing the certification bodies' candidate guides. Different results may be given in the case when examine the training materials, the courses description, and the exams material.

Overall, the conclusion that can be drawn here is that even when there are two certifications which are mapped to one ECSF profile, the actual coverage regarding the tasks, the skills and the knowledge could vary. Therefore, it is derived that training candidates may be blurred by this situation, as they do not own tools or insights for extracting concise conclusions on the domain / tasks coverage.

2.2 EU Certification Bodies

2.2.1 European Digital Infrastructure Consortium (EDIC)

European Digital Infrastructure Consortium (EDIC) is an instrument made available to Member States under the Digital Decade Policy Programme 2030 to speed up and simplify the setup and implementation of multi-country projects. EDICs will enable the achievement of the Digital Decade general objectives and targets.

Each EDIC is a legal person established by a Commission decision upon the application of at least three Member States and Commission approval. The founding Member States define the EDIC´s governance structure and other functioning rules in the Statutes. Its budget will be based on its members' contributions complemented by other sources of revenues, which may include EU and national grants. The seat of an EDIC is in a participating Member State and its legal personality must be recognised by all Member States.

An EDIC may implement a multi-country project by deploying joint infrastructure, delivering services, and bringing together – as considered appropriate by the founding Member States – public entities, private entities, final users, and industry. EDICs combine a number of benefits for projects in the area

of digital, which go beyond research. For instance, Member States hold the majority of votes in the members' assembly, which gives them a decisive role in the governance of each EDIC.[10]

An example of an EDIC is the **Cybersecurity Skills Coalition (CSC-EDIC)**, which is a planned EDIC that is expected to be established to address the EU's growing cybersecurity skills gap and promote long-term strategic cooperation between public authorities, industry, and research. While the CSC-EDIC is in the formal application stage, its objectives include pooling resources, developing cutting-edge cybersecurity capabilities, stimulating the deployment of European cybersecurity solutions, and supporting the creation of a skilled workforce through targeted training and skill alignment.[11,12]

The CSC-EDIC[13] intends to contribute to addressing cybersecurity skills gap in Member States, thereby reinforcing the competitiveness, growth, and resilience of the EU. This commitment is set out in the Communication of the Commission to the European Parliament and the Council 'Closing the cybersecurity talent gap to boost the EU's competitiveness, growth, and resilience ('**The Cybersecurity Skills Academy**'[14]). The CSC-EDIC will be dedicated to supporting key organisations, including the European Commission, European Union Agency for Cybersecurity (ENISA), and the European Cybersecurity Competence Centre (ECCC), in the effective implementation of the Cybersecurity Skills Academy initiative. The CSC-EDIC also aims to carry out proactive actions to promote the upskilling and reskilling of professionals, with a particular emphasis on the needs of Small and Medium Size Enterprises (SMEs) and public administrations in the area of cybersecurity. The CSC-EDIC will help develop competencies that align with emerging market needs, focusing on cybersecurity skills that address the requirements of recently adopted EU legislation and initiatives, including the NIS2 Directive, the Cyber Resilience Act and the European Action Plan on the Cybersecurity of Hospitals and Healthcare providers.

2.2.2 European Cybersecurity Competence Centre (ECCC)

The European Cybersecurity Competence Centre (ECCC)[15] aims to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres to build a strong cybersecurity community. The European Cybersecurity Competence Centre (ECCC), together with the Network of National Coordination Centres (NCCs), is Europe's new framework to support innovation and industrial policy in cybersecurity. This ecosystem will strengthen the capacities of the cybersecurity technology Community, shield our economy and society from cyberattacks, maintain research excellence, and reinforce the competitiveness of EU industry in this field. The ECCC will play a key role in delivering on the ambitious cybersecurity objectives of the Digital Europe Programme (DEP) and Horizon Europe programmes.

The ECCC contributes to cybersecurity training by the following means:

1. **Supporting Education and Training Programs through Funding**

   The ECCC allocates funding for various cybersecurity projects, including those that involve training and education. This support helps to create training programs for cybersecurity professionals, researchers, and the broader workforce. These programs often focus on enhancing the practical skills needed to address emerging cyber threats.

[10] https://digital-strategy.ec.europa.eu/en/policies/edic
[11] https://www.wto.org/library/events/event_resources/ecom_17072025/868_2737.pdf
[12] https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0290
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0207
[15] https://cybersecurity-centre.europa.eu

2. **Cybersecurity Skills and Workforce Development**

   The ECCC promotes the development of a cybersecurity-skilled workforce by focusing on skills gaps and enhancing education systems at all levels. This includes supporting both higher education and vocational training programs.

3. **Cybersecurity Competence Networks**

   The ECCC helps create a network of national cybersecurity competence centres (one in each EU member state) that support the delivery of cybersecurity training at the national level. These centres (e.g., the Joint Research Centre - JRC) also work with other EU-level initiatives, providing a hub for training, research, and collaboration.

4. **Promoting Cybersecurity Awareness and Awareness Campaigns**

   The ECCC also supports campaigns aimed at increasing cybersecurity awareness at all levels, including through specific training events, workshops, and public education campaigns. These campaigns often target the public, students, SMEs, and specific industries like healthcare, energy, and finance.

5. **Cybersecurity Incident Response and Exercises**

   The ECCC funds programs related to cybersecurity incident response and simulation exercises. This includes the creation of Cybersecurity Competence Networks and cyber range platforms where professionals can practice real-world scenarios.

6. **Cybersecurity Competitions and Challenges**

   To promote skills development, the ECCC supports cybersecurity challenges and capture the flag (CTF) competitions. These events are designed to stimulate innovation, foster collaboration, and improve the practical skills of participants in solving real-world cybersecurity problems.

7. **Support for Public Sector Cybersecurity Training**

   The ECCC also plays an essential role in improving the cybersecurity posture of public sector institutions across Europe. This includes training for national governments, local authorities, and public institutions on topics like cyber resilience, data protection, and incident handling.

Some direct ECCC cybersecurity training initiatives are the 'Traineeship Programme' and the 'Strengthening the cybersecurity ecosystem'.

2.3 Member-States' National Cybersecurity Strategies

National Cybersecurity Strategies (NCSS) constitute the primary policy instruments through which **European Union (EU)** and **European Free Trade Association (EFTA)** Member States articulate their strategic objectives, priorities, and governance arrangements for cybersecurity at national level. Over the past decade, the adoption and periodic revision of NCSS has been actively promoted at European and international level, with the aim of fostering coherent, risk-based, and sustainable approaches to cybersecurity governance across public and private sectors[16,17].

Beyond the articulation of high-level cybersecurity objectives, NCSS increasingly function as coordination frameworks that shape national approaches to implementation across multiple domains, including risk management, incident response, capacity building, skills development, and regulatory measures. As such, they provide a critical reference point for examining how Member States

[16] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[17] https://ncsguide.org/wp-content/uploads/2025/12/NCS-guide-2021.pdf

conceptualise and address cybersecurity training and, more specifically, training-related certification within their national cybersecurity ecosystems.

Within this context, the current section examines Member States' NCSS through a structured and analytical approach, focusing on the extent to which training-related certification is reflected in strategic objectives, selected policy instruments, and governance arrangements. The analysis is grounded in the EU regulatory context, international guidance on national cybersecurity strategies, and a comparative review of national strategy documents, with the aim of identifying common patterns, divergences, and gaps across Europe.

2.3.1 EU Cybersecurity Act and National Cybersecurity Strategies

National Cybersecurity Strategies (NCSS) are developed at national level by EU and EFTA countries, while increasingly reflecting common policy orientations established within the EU cybersecurity regulatory framework. Within this regulatory framework, the EU Cybersecurity Act[9] constitutes a key horizontal reference for Member States, particularly with regard to cybersecurity capacity building, skills development, and training. Although the Act does not mandate the adoption of specific national training programmes, it explicitly recognises that the effectiveness of cybersecurity policies and measures depends on the availability of adequately trained personnel across both public and private sectors.

The EU Cybersecurity Act assigns ENISA a formal role in supporting Member States in the area of cybersecurity training and education. This includes contributing to the development and dissemination of training materials, addressing training needs of public authorities, promoting "train-the-trainer" approaches, and facilitating coordination and exchange of good practices related to cybersecurity education and awareness[18]. These provisions establish training as a structural component of EU cybersecurity policy and implicitly guide the content and priorities of NCSS.

In this context, training-related certification emerges in the EU Cybersecurity Act as a means of ensuring that individuals performing cybersecurity-related roles possess appropriate qualifications and competences. The Regulation explicitly requires that persons involved in cybersecurity assessment and assurance activities demonstrate sound technical and vocational training, adequate knowledge of applicable requirements and standards, and the ability to document and substantiate their professional competence[9]. While the Act does not define concrete certification schemes for training, it sets clear expectations regarding the quality, credibility, and verifiability of cybersecurity-related training outcomes.

As a result, NCSS increasingly attempt to address training-related certification as part of broader workforce development and capacity-building objectives. This includes the promotion of recognised training pathways, professional qualifications, and continuous professional development mechanisms for cybersecurity practitioners, trainers, and other relevant stakeholders. Through these provisions, the EU Cybersecurity Act contributes to a more coherent treatment of cybersecurity training across Member States, while allowing NCSS to adapt implementation approaches to their specific institutional, educational, and labour-market contexts.

2.3.2 The ITU National Cybersecurity Guide as an Analytical Reference for NCSS Assessment

The *ITU Guide to Developing a National Cybersecurity Strategy*[8] provides a structured reference framework for the design, implementation, and evaluation of National Cybersecurity Strategies. It outlines overarching principles, focus areas, and good practices that support the identification of policy instruments and implementation measures, including those related to training, capacity building, and certification.

[18] https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

During the preparation of this deliverable, the 3rd Edition of the *Guide to Developing a National Cybersecurity Strategy* was published[19], introducing a refined conceptual emphasis on skills development, workforce capacity, and institutional capabilities. While the 3rd Edition does not retain the same explicit, numbered references to certification as a discrete policy instrument, it reinforces the role of training and skills as foundational enablers of strategy implementation, monitoring, and long-term sustainability. In particular, it frames cybersecurity skills and training as integral components of national capability building and strategy execution, rather than as standalone measures. This evolution of the guide enriches the interpretation of the findings presented in this subsection by highlighting a broader, ecosystem-oriented perspective on capacity development. Nevertheless, the 2nd Edition[8] remains more suitable for the purposes of this analysis, as it provides clearly identifiable paragraphs that allow a structured and comparable assessment of training-related certification provisions across NCSS.

For the purposes of this analysis, the 2nd Edition of this Guide[8] was used not as a prescriptive benchmark, but as a common analytical lens through which training-related and certification-related elements of NCSS could be consistently identified and compared across countries. In particular, **eight specific principles** were selected from the guide, as they explicitly reference certification, training, workforce development, or the use of policy instruments that may encompass training-related certification mechanisms. These principles are as follows[8]:

1. **Principle 4.7 ('Appropriate set of policy instruments')**, which establishes certification and education programmes as legitimate policy instruments alongside legislation, regulation, and standardisation. This principle is relevant as it frames training and certification not as isolated measures, but as tools that can be strategically deployed to influence stakeholder behaviour and improve national cybersecurity outcomes.
2. **Focus Area 5.2 ('Risk management in national cybersecurity')** is included to assess whether national strategies embed training and certification within a broader, lifecycle-oriented risk management approach.
3. Within this focus area, **paragraph 5.2.3 ('Identify a common methodology for managing cybersecurity risk')** explicitly refers to the use of certification programmes as supporting mechanisms for consistency, accountability, and improvement of compliance. Although primarily risk-oriented, this paragraph is relevant insofar as training and skills development underpin the effective application of any common risk management methodology.
4. **Paragraph 5.2.5 ('Establish cybersecurity policies')** is selected because it links certification to national policy frameworks for critical entities, including governance, operational practices, and minimum standards. This paragraph allows the assessment of whether training-related certification is addressed as part of formal national cybersecurity policies rather than through ad hoc or fragmented initiatives.
5. **Focus Area 5.5 ('Capability and capacity building and awareness raising')** directly addresses the human dimension of cybersecurity. It recognises that technological and regulatory measures alone are insufficient without sustained investment in skills, awareness, and institutional capacity.
6. **Paragraph 5.5.3 ('Stimulate capacity development and workforce training')** is particularly central to this analysis, as it explicitly promotes cybersecurity training schemes and the certification of security professionals at national and international level. Therefore, this paragraph serves as the primary reference point for identifying training-related certification in NCSS.
7. **Focus Area 5.6 ('Legislation and regulation')** covers the development of a legal and regulatory framework to protect society against cybercrime and promote a safe and secure cyber environment. Such a framework should define illegal cyber activities, provide tools for investigation and prosecution (including cross-border cooperation), establish compliance and

[19] https://ncsguide.org/ncs-guide-2025/

enforcement mechanisms, strengthen institutions, and support international cooperation. It must align with national, regional, and international human rights obligations.

8. **Paragraph 5.6.1 ('Establish a domestic legal framework for cybersecurity')** is included to capture the extent to which cybersecurity training and certification are embedded within national legal or regulatory frameworks. This paragraph enables the identification of strategies where *cybersecurity training-related certification* is supported by formal mandates, institutional responsibilities, or enforcement mechanisms, rather than remaining purely aspirational.

Together, these principles and focus areas provide a coherent analytical structure that reflects the full policy spectrum addressed by NCSS, ranging from the selection of policy instruments and risk management approaches to capacity building and regulatory embedding. Their combined use enables a focused and conceptually consistent examination of how training-related certification is positioned within national cybersecurity strategies, while remaining aligned with internationally recognised guidance on NCSS design and implementation.

2.3.3 Methodological Approach to the Analysis of NCSS

The analysis followed a structured qualitative methodology to identify, classify, and assess the training-related certification provisions within the NCSS of EU and EFTA countries. The methodological baseline was built on the following five authoritative sources:

1. The **ENISA NCSS Interactive Map**, as the primary inventory of NCSS documents and objectives[7]
2. The **ITU Guide to Developing a National Cybersecurity Strategy** (2nd Edition), as the main analytical reference for strategy content and policy instruments[8]
3. The **ENISA National Capabilities Assessment Framework**, for capability-oriented framing[20]
4. The **ENISA good practices on innovation under NCSS**, to support interpretation of common national measures[21]
5. The **EU Cybersecurity Act (Regulation (EU) 2019/881)**, as the relevant EU-level regulatory context[9]

Moving forward, the methodology is comprised by four steps:

Step 1: The analysis commenced with the *EU Cybersecurity Act*[9], screening for explicit references to training, education, and training-related certification (i.e., certification connected to skills development, competence building, or training delivery). Relevant passages were identified and then reviewed to confirm relevance to training capacity and competence-related measures. This step served to ground the NCSS analysis in the broader EU policy context that can influence national strategies.

Step 2: Similarly, the *ITU National Cybersecurity Strategy Guide*[8] was examined to extract strategy elements where certification and training are positioned as policy instruments and implementation enablers. In particular, references were collected from the guide's overarching principles and focus areas dealing with policy instruments, risk management, capacity building and workforce development, and legislation/regulation. From this, **a consistent set of eight checks was defined** (i.e., paragraphs 4.7, 5.2 / 5.2.3 / 5.2.5, 5.5 / 5.5.3, 5.6 / 5.6.1) to be used as the common assessment framework across EU Member States and EFTA countries.

Note: As mentioned in section 2.3.2, during the preparation of this deliverable, the 3rd Edition of the *ITU Guide to Developing a National Cybersecurity Strategy* was published[10]. The updated edition places increased emphasis on implementation, monitoring, and the evolutionary lifecycle of national strategies, with a stronger focus on operationalisation, maturity, and dynamic skills ecosystems. While these

[20] https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework
[21] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

developments reflect important advances in international guidance, the 2nd Edition of the ITU Guide[8] was retained as the primary analytical reference for this analysis. This decision was motivated by two considerations. *First*, all the assessed NCSS were created prior the 3rd Edition of the ITU Guide publication. *Second*, the 2nd Edition of the ITU Guide provides a more explicit and structured articulation of principles, focus areas, and good practices, including clearly identifiable references to training, certification, and capacity-building measures. These characteristics make it more suitable as a stable and transparent analytical framework for comparative assessment across Member States, ensuring methodological consistency, comparability of results, and traceability of findings, while the conclusions of the analysis remain aligned with the broader strategic directions reinforced in the 3rd Edition.

Step 3: Next, the *ENISA NCSS Interactive Map*[7] objectives were reviewed to determine which objectives are inherently training or skills-related (e.g., awareness, cyber hygiene, skills gap), and to contextualise how such objectives are expected to appear in NCSS. Since common ground with the scope of work was found, and therefore relevant expectations from the NCSS exist, then each NCSS was assessed against the aforementioned eight principles as taken from the ITU National Cybersecurity Strategy Guide[8] to ensure consistent cross-country comparability.

Step 4: Then, findings were recorded using a simple three-level qualitative scoring scale (i.e., YES / PARTIAL / NO). This approach was chosen to ensure consistency, transparency, and cross-country comparability, while accounting for the heterogeneity of NCSS structure, scope, and level of detail.

A score of YES was assigned where an NCSS contains a clear, explicit, and direct reference to the examined element of the Guide, demonstrating that the strategy formally recognises the relevance of the corresponding principle or focus area at strategic level. For **training-related certification**, a YES requires an explicit textual link between cybersecurity training or skills development and certification, professional qualification, or formal competence validation of cybersecurity professionals. The presence of implementation details, operational mechanisms, or action-level specifications was not required, as NCSS are strategic documents rather than implementation plans.

A score of PARTIAL was assigned where the examined element is referenced only indirectly, implicitly, or in a fragmented manner, without a clear or explicit strategic recognition. This includes cases where training, skills development, or capacity building are mentioned in general terms, but **without an explicit connection to certification or formal competence validation**, or where relevant concepts appear sporadically without being positioned as part of the strategy's core objectives or policy instruments.

A score of NO was assigned where no relevant reference could be identified in the NCSS with respect to the examined element of the Guide. This includes cases where the strategy is silent on the topic, or where references are limited to adjacent concepts that cannot reasonably be interpreted as addressing the specific principle or focus area under assessment.

The YES / PARTIAL / NO scheme does not aim to measure the overall quality, maturity, or effectiveness of a national cybersecurity strategy. Instead, it serves as an analytical tool to identify the presence, clarity, and degree of formalisation of specific training- and certification-related aspects, as defined by the selected reference points of the ITU National Cybersecurity Strategy Guide. This qualitative approach allows meaningful comparison across strategies while avoiding over-interpretation or artificial quantification of heterogeneous policy documents.

2.3.4 Results of the NCSS Analysis

Following the assessment methodology which is described in section 2.3.3, we gather our findings in Table 4.

Table 4. Assess training-related certification provisions within the NCSS of EU and EFTA countries

No.	Country	EU / EFTA	NCSS Year	ITU National Cybersecurity Strategy Guide's References							
				4.7	5.2	5.2.3	5.2.5	5.5	5.5.3	5.6	5.6.1
1	Austria[22]	EU	2021	YES	YES	NO	NO	YES	NO	YES	PARTIAL
2	Belgium[23]	EU	2024	YES	YES	NO	YES	YES	NO	YES	YES
3	Bulgaria[24]	EU	2021	YES	YES	NO	NO	YES	NO	YES	NO
4	Croatia[25]	EU	2015	YES	YES	PARTIAL	YES	YES	NO	YES	PARTIAL
5	Cyprus[26]	EU	2020	YES	YES	NO	YES	YES	NO	YES	PARTIAL
6	Czech Republic[27]	EU	2021	YES	YES	NO	YES	YES	NO	YES	YES
7	Denmark[28]	EU	2022	PARTIAL	YES	NO	YES	YES	NO	YES	PARTIAL
8	Estonia[29]	EU	2024	YES	YES	YES	YES	YES	NO	YES	YES
9	Finland[30]	EU	2024	YES	YES	NO	YES	YES	NO	YES	NO
10	France[31]	EU	2025	YES	PARTIAL	NO	PARTIAL	YES	NO	PARTIAL	NO
11	Germany[32]	EU	2021	YES	YES	PARTIAL	YES	YES	PARTIAL	YES	YES
12	Greece[33]	EU	2020	YES	YES	PARTIAL	YES	YES	NO	YES	PARTIAL
13	Hungary[34]	EU	2025	YES	YES	PARTIAL	YES	YES	NO	YES	PARTIAL
14	Iceland[35]	EFTA	2022	PARTIAL	YES	NO	YES	YES	NO	YES	YES
15	Ireland[36]	EU	2019	YES	YES	NO	YES	YES	NO	YES	YES
16	Italy[37]	EU	2022	YES	YES	PARTIAL	YES	YES	NO	YES	YES

[22] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/AT_NCSS_2021_en.pdf
[23] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/BE_POLICY_DOCUMENT_2024_en.pdf
[24] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/BG_NCSS_2021_en%20%28draft%20translation%29.pdf
[25] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/HR_NCSS_2015_en.pdf
[26] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/CY_NCSS_2020_en.pdf
[27] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/CZ_NCSS_2021_en.pdf
[28] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/DK_NCSS_2022_en.pdf
[29] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf
[30] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/FI_NCSS_2024_en.pdf
[31] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/FR_NCSS_2025_fr.pdf
[32] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/DE_NCSS_2021_en.pdf
[33] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EL_NCSS_2020_en.pdf
[34] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/HU_NCSS_2025_hu.pdf
[35] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/IS_NCSS_2022_en.pdf
[36] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/IE_NCSS_2019_en.pdf
[37] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/IT_NCSS_2022_en.pdf

No.	Country	EU / EFTA	NCSS Year	ITU National Cybersecurity Strategy Guide's References							
				4.7	5.2	5.2.3	5.2.5	5.5	5.5.3	5.6	5.6.1
17	Latvia[38]	EU	2023	YES	YES	NO	YES	YES	PARTIAL	YES	YES
18	Liechtenstein[39]	EU	2025	YES	YES	NO	PARTIAL	YES	NO	PARTIAL	NO
19	Lithuania[40]	EU	2018	YES	YES	NO	PARTIAL	YES	YES	YES	PARTIAL
20	Luxembourg[41]	EU	2021	YES	YES	YES	YES	YES	PARTIAL	YES	YES
21	Malta[42]	EU	2023	YES	YES	NO	YES	YES	YES	YES	YES
22	Netherlands[43]	EU	2022	YES	YES	PARTIAL	YES	YES	PARTIAL	YES	YES
23	Norway[44]	EFTA	2019	PARTIAL	YES	YES	YES	YES	NO	YES	YES
24	Poland[45]	EU	2019	YES	YES	PARTIAL	YES	YES	NO	YES	PARTIAL
25	Portugal[46]	EU	2019	YES	YES	NO	YES	YES	YES	YES	PARTIAL
26	Romania[47]	EU	2022	YES	YES	PARTIAL	YES	YES	NO	YES	YES
27	Slovakia[48]	EU	2021	YES	YES	PARTIAL	YES	YES	NO	YES	NO
28	Slovenia[49]	EU	2019	PARTIAL	NO	NO	NO	YES	NO	NO	NO
29	Spain[50]	EU	2019	YES	PARTIAL	NO	PARTIAL	YES	YES	PARTIAL	NO
30	Sweden[51]	EU	2025	YES	YES	NO	YES	YES	PARTIAL	YES	YES
31	Switzerland[52]	EFTA	2023	YES	YES	NO	PARTIAL	YES	NO	YES	PARTIAL

The application of the analytical framework described in sections 2.3.1–2.3.3 enabled **a systematic review of 31 national cybersecurity strategies** from EU and EFTA countries, assessing the extent to which training-related certification is reflected across the selected principles and focus areas of the ITU National Cybersecurity Strategy Guide. Our remarks upon the findings are as follows.

[38] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/LV_NCSS_2023_en.pdf
[39] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/LI_NCSS_2025_en.pdf
[40] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/LT_NCSS_2018_en.pdf
[41] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/LU_NCSS_2021_en.pdf
[42] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/MT_NCSS_2023_en.pdf
[43] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/NL_NCSS_2022_en.pdf
[44] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/NO_NCSS_2019_en.pdf
[45] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/PL_NCSS_2019_en.pdf
[46] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/PT_NCSS_2019_en.pdf
[47] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/RO_NCSS_2022_ro.pdf
[48] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/SK_NCSS_2021_en.pdf
[49] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/SK_NCSS_2021_en.pdf
[50] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/ES_NCSS_2019_en.pdf
[51] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/SE_NCSS_2025_se.pdf
[52] https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/CH_NCSS_2023_en.pdf

Principle 4.7 ('Appropriate set of policy instruments'). It is the most consistently addressed element across the analysed strategies. The vast majority of NCSS explicitly recognise the need to deploy a mix of policy instruments, such as regulation, education, incentives, and coordination mechanisms, to achieve national cybersecurity objectives. This widespread presence indicates a shared understanding among Member States that cybersecurity outcomes depend on behavioural change supported by appropriate institutional and policy tools. Partial coverage is observed mainly in older or more narrowly scoped strategies, where the principle is implied rather than explicitly articulated.

Focus Area 5.2 ('Risk management in national cybersecurity'). Almost all NCSS demonstrate alignment with a risk-based approach to cybersecurity governance. References to national risk assessment, prioritisation of threats, and lifecycle-oriented risk management are common, reflecting strong convergence with international good practices. However, this alignment becomes less consistent when examining ***Paragraph 5.2.3 ('Identify a common methodology for managing cybersecurity risk')***. Only a limited number of strategies explicitly refer to a common or standardised risk management methodology, and even fewer link such methodologies to certification-related mechanisms. In most cases, methodological consistency is assumed rather than formally defined, resulting in a predominance of NO or PARTIAL scores for this paragraph.

Paragraph 5.2.5 ('Establish cybersecurity policies'). It shows comparatively stronger coverage. A large number of NCSS include references to national cybersecurity policies for public authorities, critical infrastructure operators, or other key stakeholders. These policies typically address governance structures, minimum requirements, and coordination mechanisms. Nevertheless, explicit references to certification within these policy frameworks remain uneven, with several strategies addressing policy development without clearly linking it to training-related certification.

Focus Area 5.5 ('Capability and capacity building and awareness raising'). It is one of the most uniformly addressed elements across the analysed NCSS. Nearly all strategies explicitly recognise the importance of human capacity, awareness, and skills development as foundational components of national cybersecurity. This confirms a strong consensus on the centrality of the human factor within cybersecurity strategies.

Paragraph 5.5.3 ('Stimulate capacity development and workforce training'). Contrary to the Focus Area 5.5, it reveals a significant divergence in national approaches. While many NCSS refer to training programmes, education initiatives, or workforce development in general terms, only a small subset explicitly addresses the certification of cybersecurity professionals. In several cases, certification is either absent or limited to indirect references, leading to a predominance of NO and PARTIAL scores. This highlights a structural gap between the recognition of training needs and the formal validation of professional competences through certification.

Focus Area 5.6 ('Legislation and regulation'). It is widely reflected in national strategies. Most NCSS include references to the development or evolution of legal and regulatory frameworks addressing cybersecurity, cybercrime, and related institutional responsibilities. However, when narrowing the analysis to ***Paragraph 5.6.1 ('Establish a domestic legal framework for cybersecurity')***, the results show greater variation. While several strategies embed training- or certification-related aspects within legal or regulatory frameworks, many others address legislation without explicitly linking it to skills validation or professional certification.

Overall, the results demonstrate a clear pattern across Member States. Strategic recognition of training, awareness, and capacity building is widespread and well established. In contrast, training-related certification, particularly certification of cybersecurity professionals, is addressed in a fragmented and uneven manner. Differences are observed not only in the depth of treatment but also in the degree of formalisation and institutional anchoring. These findings indicate that, despite convergence at the level of strategic intent, national approaches to training-related certification remain heterogeneous, reflecting differing policy priorities, institutional capacities, and regulatory traditions across Europe.

2.3.5 Identified Gaps and Implications for Training-Related Certification in Europe

The results of the National Cybersecurity Strategies (NCSS) analysis reveal a structural discrepancy between the widespread recognition of cybersecurity training as a strategic priority and the limited, fragmented, and uneven treatment of training-related certification across Europe. While most NCSS explicitly acknowledge the importance of education, skills development, and workforce capacity, only a relatively small number treat certification as a distinct and systematic mechanism for validating cybersecurity competences.

A **first key gap** concerns the conceptual separation between training and certification. In many strategies, training is addressed primarily in terms of awareness raising, education, or upskilling, without corresponding consideration of how acquired competences are assessed, validated, or formally recognised. As a result, certification is frequently absent or referenced in broad and ambiguous terms, making it difficult to determine whether national approaches support consistent, transparent, and comparable validation of cybersecurity skills. This weak conceptual linkage limits the strategic role of certification as a policy instrument rather than a voluntary or ad hoc outcome of training initiatives.

A **second gap** relates to the limited integration of training-related certification within national governance and risk management frameworks. Despite the emphasis placed by the ITU National Cybersecurity Strategy Guide on embedding certification within risk management methodologies, cybersecurity policies, and capability requirements, only a minority of NCSS explicitly reflect such integration. In most cases, training and certification are positioned as supportive or enabling activities, rather than as structural components linked to critical roles, risk-based prioritisation, or minimum capability thresholds. This reduces their effectiveness as tools for managing systemic cyber risk at national level.

From a regulatory and institutional perspective, the analysis further indicates that cybersecurity training-related certification is rarely anchored in binding legal or policy frameworks. Few strategies define clear institutional responsibilities, quality assurance mechanisms, or continuity requirements for certification schemes. The absence of such anchoring limits not only national coherence, but also mutual recognition, comparability, and long-term sustainability of certification efforts across borders.

These gaps have direct implications at European level. The lack of a coherent and comparable approach to training-related certification across NCSS undermines the development of a shared cybersecurity skills baseline, complicates cross-border cooperation, and constrains workforce mobility within the EU and EFTA area. Moreover, it weakens the effectiveness of EU-level initiatives aimed at addressing the cybersecurity skills gap, as national strategies provide uneven and incompatible foundations for implementation.

Overall, the findings indicate that while cybersecurity training is firmly embedded in national strategic discourse, training-related certification remains underdeveloped as a strategic governance instrument. Addressing this gap cannot rely solely on further national initiatives. Instead, it points to the need for coherent European training-related certification mechanisms that complement national strategies, support comparability and trust, and align skills validation with EU-level policy objectives on cybersecurity capacity building. In this sense, the results of the NCSS analysis provide a concrete empirical basis for the subsequent sections of this deliverable, which explore how European-level approaches can strengthen the role of training-related certification within the broader cybersecurity ecosystem.

2.4 EU Initiatives towards harmonising the EU's Cybersecyrity Training Certification landscape

The **Digital Europe Programme (DIGITAL)** is an EU funding programme focused on bringing digital technology to businesses, citizens, and public administrations. The Digital Europe Programme (DIGITAL) provides strategic funding to answer these challenges, supporting projects in key capacity areas such as: supercomputing, artificial intelligence, cybersecurity, advanced digital skills, and

ensuring a wide use of digital technologies across the economy and society. It supports industry, small and medium-sized enterprises (SMEs), and public administration in their digital transformation. The total overall budget for the entire Digital Europe Programme (covering AI, cloud, data, skills, and cybersecurity) for the 2025-2027 period is around €1.3 billion.

The **European Health and Digital Executive Agency (HaDEA)** has the mission to implement actions that strengthen Europe in the domains of health, food safety, digital technologies and networks, industrial capacities and space. Among other fields of interest, HaDEA currently manages Digital Europe Programmes (DEP) in the field of cybersecurity professional training[53].

Alongside the international, EU, and Member State certification bodies previously discussed, EU-level initiatives play a pivotal role in shaping the cybersecurity training and certification landscape. As part of wider efforts to harmonise cybersecurity education and certification across Europe, these initiatives seek to establish common standards and coherent frameworks. This section explores the EU-led initiatives, assessing their influence on the certification ecosystem and their relevance to the objectives of **CyberSecPro project**.

Updating to what has been documented in the deliverable D3.2, the initiatives presented in this section contribute significantly to the development of a shared European framework for cybersecurity certification and closely align with CyberSecPro's overarching goals. They reflect a common commitment to strengthening cybersecurity training, standardisation, and workforce development within the European context. Building on this existing work, CyberSecPro aims to provide added value by focusing on the self-development of students and professionals and by bridging the gap between academic knowledge and industry-required skills. In doing so, it promotes a more coherent, comprehensive, and aligned approach to cybersecurity training and certification across Europe.

2.4.1 AKADIMOS[54]

The AKADIMOS project aims to support the creation and initial operation of the European Cybersecurity Skills Academy (henceforth "the Cyber Skills Academy" or "the Academy") which, as specified in the relevant EC Communication aims at a single point of entry that establishes synergies for cybersecurity training initiatives along with funding opportunities regarding the development of cybersecurity skills and, hence, contributing towards closing the skills gap of cybersecurity professionals across EU. AKADIMOS is a horizontal project which works towards the support and evolution of important instruments and outcomes envisioned by all pillars of the Academy, including the coordinated cooperation and involvement of all relevant stakeholders (EC, ENISA, ECCC, relevant EC-funded projects, cybersecurity training companies and industry, public entities and SMEs). The goal is to avoid scattered and redundant efforts, offering the opportunity to scale-up and make a noticeable impact in closing the cybersecurity professionals' gap. The project will enhance the European Cybersecurity Skills Framework, and will also create tools for improvement and effective monitoring of the impact of existing and future initiatives. It will create an information system for cybersecurity curricula that will contain all courses material, their metadata, the registry of Trainers, and provide Services to various entities for scale-up, and services for updating the Digital Skills and Jobs Platform and for validating content towards a solid and realistic plan for the sustainability of the Academy. The project will establish procedures for the efficient and effective decentralized operation of the Academy, towards making the Academy the unique EU reference ecosystem for cybersecurity professionals.

[53] https://hadea.ec.europa.eu/news/discover-hadea-managed-projects-cybersecurity-funded-digital-europe-programme-2025-10-17_en?utm_source=chatgpt.com
[54] https://www.cti.gr/en/ongoing-research-projects/akadimos-en/

2.4.2 CADMUS[55]

The CADMUS-project aims to address the cybersecurity expertise shortage in Europe by developing targeted training opportunities based on approaches including cyber range projects, games, hackathons, bootcamps, and traineeships. These interventions aim to upskill educators, trainers, SME and startup employees, civil servants as well as graduate students who target cybersecurity careers. The project will utilize existing initiatives and offers in cyber security training to build upon and develop enhanced training curricula based on integrating proven training models and standards. The CADMUS-project contributes to the overall Digital Europe Programmes (DEP) objectives by enhancing the quality and effectiveness of cybersecurity training across Europe, ensuring that training and education frameworks are developed, and data are aligned with both current and emerging cybersecurity needs. This alignment is crucial for effectively addressing current and future market needs and facilitating appropriate workforce reskilling, upskilling, and cross-skilling. By establishing a centralized framework for skill mismatch analysis and forecasting, the initiative aims to streamline and integrate training efforts across Europe, enhancing coordination and ensuring that all training activities and opportunities are aligned with a unified set of goals.

2.4.3 CYCERONE[56]

Cycerone, an initiative supported by the European Union in collaboration with leading universities and educational partners, is designed to address the critical need for enhanced cybersecurity skills across Europe. In an era where many organizations, particularly SMEs and public administrations, face significant challenges due to a skills gap in cybersecurity, Cycerone seeks to empower these entities to protect themselves against the growing landscape of cyber threats. Cycerone aims to bridge this gap by offering tailored and free cybersecurity training programs strategically designed to provide employees with the essential knowledge and tools required to develop and sustain secure digital infrastructures.

2.4.4 CYBERPRO TRAIN[57]

The CyberPro Train project addresses the critical cybersecurity skills shortage in the European Union by developing an innovative, scalable education and training model tailored for professionals in SMEs and public administrations. It aims to bridge the cybersecurity skills gap through specialized training programs that combine both theoretical and practical knowledge, in alignment with the EU's Digital Europe Programme objectives. The project supports key EU cybersecurity directives, such as the NIS2 Directive and Cyber Resilience Act, and is designed to prepare a new generation of cybersecurity professionals to protect critical infrastructures and respond effectively to cybersecurity threats. In the longer term, CyberPro Train promotes a collaborative and standardized approach to cybersecurity training across EU member states, aligning with the goals of the European Commission's Cybersecurity Skills Academy. By creating a unified, scalable training model and encouraging partnerships, the project facilitates knowledge sharing and collective growth within the cybersecurity community, ensuring that the EU can effectively respond to new and complex cyber threats.

2.4.5 CyberSec4OT[58]

The CyberSec4OT project reflects both the urgency and strategic importance of cybersecurity within industrial and operational technology (OT) environments. As the digital transformation of European industry accelerates, particularly with the adoption of Industry 4.0 technologies, OT systems—which control physical processes in sectors such as manufacturing, energy, and transportation—are becoming increasingly integrated with traditional IT infrastructure. While this convergence enables new efficiencies and capabilities, the project also introduces a host of cybersecurity vulnerabilities that can

[55] https://cadmus-project.eu/
[56] https://cycerone.eu
[57] https://cyberprotrain.eu/
[58] https://cysec4ot.com/

impact not only business operations but also critical infrastructure and public safety. To meet these growing challenges, CyberSec4OT brings together 10 organizations across 5 European countries, forming a multidisciplinary partnership that combines deep expertise in cybersecurity, industrial systems, education, and policy. The project's core objective is to strengthen Europe's resilience by building a well-trained, highly competent OT cybersecurity workforce capable of addressing the complex threats that arise in digital industrial environments. Recognizing the unique cybersecurity requirements of OT, where downtime or malfunction can have serious physical and economic consequences, CyberSec4OT aims to deliver training programs that are both technically rigorous and grounded in real-world industry needs. One of the project's key innovations is the development of tailored, modular training content that spans a range of proficiency levels and job roles. These programs are supported by the establishment of cyber ranges and hands-on laboratories, where learners can engage in simulated attack-defense scenarios and gain practical experience using the latest tools and techniques. To ensure widespread accessibility, CyberSec4OT is also creating a comprehensive Digital Learning Hub, which will house all training materials, interactive modules, and best-practice toolkits in a multilingual, user-friendly format.

2.4.6 CYRUS[59]

The goal of the CYRUS project is to propose a novel training programme to develop a cybersecurity innovation DNA and support companies in transport and manufacturing to respond to and mitigate cyber threats and attacks. Starting from the analysis of current needs and future cyber threat scenarios the project creates personalised cybersecurity training and assessment methodology for employees and professionals in the two sectors. The CYRUS project designs and implements cybersecurity training courses to improve the cybersecurity skills of all-level employees and give them the means to identify and mitigate cyber threats. The project courses are focused on: cybersecurity technical skills; cybersecurity methodological and organisational aspects; practical exercises; on-the-job simulations in a cyber-range environment for the different industrial sectors.

2.4.7 NERO[60]

NERO is an advanced Cybersecurity Ecosystem designed to address the distinct aspects of awareness, training, and education in cybersecurity. NERO not only provides tools and resources but also focuses on cultivating a culture of cybersecurity awareness and resilience among organisations and individuals. The NERO project aims to enhance the cybersecurity posture of European SMEs. A crucial aspect of this initiative is the development and delivery of a training program designed to raise cybersecurity awareness and bridge the cybersecurity skill gap among small and medium enterprises within the EU. The project's comprehensive curriculum covers a range of cybersecurity topics, from fundamental concepts to advanced principles, specifically tailored towards SMEs. Furthermore, specialised training sessions on NERO tools are provided to enable SMEs to seamlessly integrate these tools into their operations.

2.4.8 BioNT[61]

BioNT, the Bio Network for Training, is an international consortium of nine partners, including six academic entities and three SMEs. The vision of the consortium is to provide a high-quality training program and community for digital skills relevant to the biotechnology industry and biomedical sector. The BioNT project's training model designed by the project proponents encodes the following missions:

[59] https://cyrus-project.eu/
[60] https://nerocybersecurity.eu/
[61] https://biont-training.eu/

To provide high-quality courses in the context of two coherently designed curricula; To have a beneficial impact not only on the course participants; To ensure the community and activities sustainability beyond the project duration.

Despite the fact the BioNT project does not cover the field of cybersecurity training in particular, it copes with the issue of the trainees certification by issuing micro-credentials at the training completion level. It also provides to training course providers an element list to check the micro-credentials requirements.

2.4.9 EURIDICE[62]

EURIDICE stands for EURopean Inclusive Education for Digital Society, Social Innovation, and Global CitizEnship. Its overall objective is to educate and build in an interdisciplinary way the coming generation of social innovators with advanced digital technologies, with an emphasis on the highly societally influential sectors of Education, Communication and Culture.

Again, this project does not cover the field of cybersecurity training in particular. However, the project proposes an assessment method of non-academic, non-accredited courses which focuses on the micro-credentials approach. The EURIDICE approach includes the establishment of a so-called micro-credential Board of academic senior experts from universities. Then, they follow a specific pathway for eventually handing out to training providers the right to add to the certificates they issue a EURIDICE-level "stamp", as it were: EURIDICE Quality-Assured micro-credential. That board inspects any submitted course on the grounds of the requirements defined by the Council of Europe in 2022 regarding the micro-credentials.

2.4.10 DIS4SME[63]

DIS4SME delivers different types of courses responding to the real needs of SMEs in terms of data interoperability, especially on location data interoperability, to cover state-of-the-art technological as well as policy trends. The project designs and delivers short-term training courses for upskilling and reskilling of the labour force, with a particular focus on SMEs owners, managers, and employees.

Again, the DIS4SME does not cover the field of cybersecurity training in particular. Nevertheless, it copes with the challenge to identify a cost-effective and reliable system for issuing digital micro-credentials compliant with the EU Recommendation on micro-credentials. To address this issue constraints, the DIS4SME project adopted the European Digital Credentials Infrastructure (EDCI) Issuer, an official tool provided by the EU, for issuing micro-credentials in a free and secure manner by facilitating an e-seal.

2.4.11 Skillnet Ireland[64]

The Skillnet Ireland is built on a national framework of business networks. These networks act as intermediaries between enterprises and training providers, fostering collaboration, and ensuring that training programmes are demand-driven and aligned with both sectoral and national priorities. Rather than relying solely on traditional education systems, the model empowers businesses—particularly SMEs—to identify critical skills gaps and co-develop training solutions that often lead to recognised accreditation. Business networks facilitate engagement across diverse sectors, reduce administrative burden, and support access to micro-credentials, recognition of prior learning (RPL), and formal qualifications. They also enable real-time intelligence gathering by maintaining close contact with employers, allowing for agile and targeted responses to emerging trends.

[62] https://euridice.eu/
[63] https://www.dis4sme.eu
[64] https://www.skillnetireland.ie/

One of the main outcomes of Skillnet Ireland in the increased alignment between industry and accreditation. This outcome is twofold: Bridged the gap between industry needs and education offerings, resulting in more job-ready; Enabled the mainstreaming of micro-credentials and flexible learning pathways—recognised increasingly in formal systems graduates and upskilled employees.

2.5 EU Challenges in Certifying Cybersecurity Training

In this chapter, the political and policy related, legal, technical, standard-related, human-related challenges for the harmonisation, interoperability, and compliance of cybersecurity training in EU are presented.

2.5.1 Certification of Training Completion *versus* Validation of Skills and Knowledge

When viewed through the lens of the European Cybersecurity Skills Framework (ECSF), the difference between **certification of training completion** (usually mentioned as 'certificates of completion') and **certification of persons** (validation of skills and knowledge) becomes not only clearer, but structural and non-negotiable. ECSF explicitly models professional capability, whereas the training completion evidences learning activity.

The following text discusses[65,66,67,68,69] on this issue through the lens of the ECSF perspective.

1. **What Is Being Recognised?**
   1.1. ***Training Completion***
   - Recognises exposure to learning content
   - Is not mapped to an ECSF professional profile
   - Does not demonstrate achievement of ECSF:
     - Tasks
     - Responsibilities
     - Outcomes
     - Proficiency levels

From an ECSF standpoint, a training certificate answers only to the question "*Has this person followed a learning pathway related to cybersecurity*?"

1.2. Certification of Persons

- Recognises demonstrated professional competence
- Is explicitly aligned to:
  - An ECSF professional profile
  - A defined ECSF proficiency level
- Confirms ability to:
  - Perform ECSF-defined tasks
  - Deliver ECSF-defined outcomes
  - Exercise responsibility and autonomy appropriate to the level

[65] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
[66] https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf
[67] https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf
[68] https://digital-skills-jobs.europa.eu/en/inspiration/resources/european-cybersecurity-skills-framework-ecsf
[69] https://esco.ec.europa.eu/en/about-esco/publications/publication/crosswalk-between-esco-and-european-cybersecurity-skills

From an ECSF standpoint, certification of persons answers: "*Can this person perform the ECSF role at the stated level in a professional context?*"

2. Role Alignment

If no ECSF role and level are claimed, then no professional competence is being validated. Table 5 contrasts the training completion and the certification of persons through various ECSF aspects.

Table 5. Distinction between training completion and certification of persons under the ECSF scope

Aspect	**Training Completion**	**Certification of Persons**
ECSF profile	Not required	Mandatory
ECSF tasks	Referenced informally or partially	Explicitly assessed
ECSF level	Not defined	Explicitly stated
Role boundaries	Undefined	Clearly enforced

3. Competence vs Learning Outcomes

As derived from the ECSF, competence is measured by *what the person can do*, not *what they have learned*. The following text contrasts these two terms (i.e., learning outcome and competence).

3.1. Training Completion

- Learning outcomes describe:
  - What was taught
  - What was covered
- There is no requirement to demonstrate:
  - Autonomous execution
  - Decision-making under constraints
  - Responsibility for outcomes

3.2. Certification of Persons

- Competence outcomes derive directly from ECSF:
  - Role purpose
  - Tasks and deliverables
  - Skill and knowledge expectations
- Demonstration of:
  - Correct execution (lower ECSF levels)
  - Judgment and accountability (higher ECSF levels)

4. Assessment Implications

4.1. Training Completion

- Assessment (if any) is:
  - Attendance-based or formative
  - Designed to support learning
- Failure is uncommon and often avoided

4.2. Certification of Persons

- Assessment must be:
  - Independent
  - Outcome-oriented
  - Proportionate to ECSF level
  - Failure is expected and acceptable

Example:

ECSF Level 2 → structured exams and guided labs

ECSF Level 4 → scenario-based evaluation, portfolio review, peer validation

A multiple-choice exam alone cannot validate ECSF Level 3 or 4 competence.

5. **Responsibility and Autonomy**

ECSF differentiates roles primarily by:

- Degree of autonomy
- Decision-making authority
- Accountability for outcomes

Therefore, training completion certificates cannot claim ECSF-level responsibility without misrepresentation. Table 6 contrasts how autonomy, responsibility, and professional judgement apply to training completion and to certification of persons.

Table 6. Responsibility and Autonomy under training completion and certification of persons

Aspect	**Training Completion**	**Certification of Persons**
Autonomy	Not assessed	Explicitly assessed
Responsibility	Not claimed	Core validation element
Professional judgment	Not evaluated	Mandatory at higher ECSF levels

6. **Portability and Recognition**

ECSF-aligned certification of persons enables **cross-border recognition**; training certificates do not. Table 7 contrasts how portability and recognition apply to training completion and to certification of persons.

Table 7. Portability and Recognition under training completion and certification of persons

Aspect	**Training Completion**	**Certification of Persons**
ECSF portability	None	High
Employer interpretability	Low	High
Regulatory usability	Limited	Strong

7. **Complementary Roles in an ECSF-Based System**

ECSF implicitly positions training and certification as **distinct but complementary**:

- Training → prepares individuals to acquire ECSF competencies
- Certification of persons → validates ECSF competencies independently

A mature ECSF-aligned ecosystem always separates these functions.

8. **Market Meaning and Risk**

- Training completion certificates:
  - Signal awareness or upskilling
  - Do not qualify a person for an ECSF role
- Certification of persons:
  - Signals job-ready capability for a defined ECSF role and level

Mislabelling training certificates as “certifications”:

- Undermines ECSF comparability
- Creates false confidence for employers
- Weakens trust in the cybersecurity labor market

Concluding this section, Table 8 summarises the distinction between the certificates of training completion and the certification of persons.

Table 8. ECSF-based distinction between the certificates of training completion and the certification of persons

Dimension	**Training Completion**	**Certification of Persons**
ECSF role	None	Explicit
ECSF level	None	Explicit
Focus	Learning activity	Professional competence
Assessment	Formative or minimal	Independent and summative
Market claim	“Has learned”	“Can perform”

2.5.2 Challenges and EU Efforts

Providing cybersecurity training certifications entails addressing a range of structural and operational challenges, largely driven by the dynamic nature of the cybersecurity domain and the continuously evolving threat landscape. Certification schemes must operate in an environment characterised by rapid technological change, increasing role specialisation, and heightened expectations regarding professional competence and trust.

One of the principal challenges is the **pace of technological evolution**. Cybersecurity technologies, tools, and methodologies evolve rapidly, requiring certification programmes to undergo frequent updates to remain relevant and effective. Failure to maintain currency risks certifying professionals with outdated or insufficient skills.

A further challenge arises from the **breadth and diversity of cybersecurity specialisations**. The field encompasses multiple distinct professional domains, such as penetration testing, incident response, digital forensics, governance, risk management, and compliance. Designing certification schemes that adequately reflect this diversity while maintaining sufficient depth and role clarity remains complex.

The **continuous emergence of new cyber threats and attack techniques** further complicates certification design. Certification schemes must be sufficiently agile to incorporate emerging threat vectors, adversarial tactics, and defensive practices, ensuring that certified professionals are equipped to address contemporary and foreseeable risks.

Cybersecurity is inherently a **practice-oriented discipline**, making the integration of hands-on experience a critical requirement. Developing assessments that realistically simulate operational environments—such as incident response scenarios or system hardening exercises—poses significant logistical and technical challenges but is essential for validating real-world competence.

Certification schemes must also demonstrate **global relevance and recognition**. Given the cross-border nature of cyber threats, certifications are expected to align with international standards and frameworks, enabling portability and recognition across jurisdictions. Achieving such alignment while respecting regional regulatory requirements presents an ongoing challenge.

The **recognition, integrity, and governance of certification bodies** constitute another critical dimension. Certification providers must operate within established legal, financial, and standardisation frameworks to ensure credibility and impartiality. At the same time, cost and accessibility considerations

must be addressed to avoid excluding small and medium-sized enterprises (SMEs), micro-enterprises (MEs), and individuals from certification pathways.

Maintaining an appropriate **balance between theoretical knowledge and practical skills** is also essential. Certification schemes must ensure that candidates possess both a robust conceptual understanding of cybersecurity principles and the capability to apply them effectively in operational contexts.

Certification standards themselves must remain **adaptive and forward-looking**. Regular review and revision of certification criteria, learning outcomes, and assessment methods are required to reflect evolving industry needs and regulatory expectations.

Finally, **credibility and trust** are foundational to the value of cybersecurity certifications. Transparent governance structures, rigorous assessment processes, ethical requirements, and clearly articulated competence claims are necessary to sustain confidence among employers, regulators, and the wider market.

At the policy level, the **European Union (EU)** has undertaken significant initiatives to promote cybersecurity awareness, skills development, and professional training. Central to these efforts is the **European Cybersecurity Strategy**, which emphasises the development of a resilient and skilled cybersecurity workforce as a strategic priority for the Union.

The **Directive on Security of Network and Information Systems (NIS Directive)** establishes a legislative framework aimed at achieving a high common level of cybersecurity across Member States. It explicitly encourages the development of national strategies that include measures to strengthen cybersecurity skills and professional competences.

The establishment of the **European Cybersecurity Competence Centre (ECCC)** further reinforces the EU's commitment to enhancing cybersecurity capabilities, including through coordination and support of training, education, and skills development initiatives at Union level.

Complementing these efforts, the **Digital Education Action Plan** seeks to strengthen digital skills and competencies across society, recognising digital literacy as a foundational element of cybersecurity preparedness. Awareness-raising initiatives such as the **European Cybersecurity Month (ECSM)** further contribute to building a cybersecurity-aware culture among citizens and organisations.

The EU also supports cybersecurity skills development through **dedicated funding programmes**, including the Digital Europe Programme (DEP), which provides financial support for training, education, and innovation in cybersecurity.

The **European Skills Agenda** underscores the importance of lifelong learning and digital skills development, addressing workforce shortages and skills mismatches that directly affect the cybersecurity sector.

A key structural contribution is the **European Cybersecurity Skills Framework (ECSF)**, which defines twelve cybersecurity professional profiles, each articulated in terms of responsibilities, required skills and knowledge, and interdependencies. The ECSF provides a common reference point for aligning training, certification, and workforce development initiatives across the EU.

Additional policy instruments, such as the **EU Cyber Solidarity Act**[70], include provisions related to cybersecurity training and preparedness, including the establishment of a **European Cyber Shield** based on a coordinated network of Security Operations Centres (SOCs) across Member States.

The proposed **Cybersecurity Skills Academy** aims to consolidate public and private initiatives related to cybersecurity skills development, providing structured access to training, scholarships, and certifications for individuals pursuing cybersecurity careers.

Finally, proposed amendments to the **Cybersecurity Act**, including the establishment of a certification scheme for managed security services, as well as related Council Recommendations on digital skills development, further illustrate the EU's holistic and policy-driven approach to addressing cybersecurity skills shortages and strengthening professional capacity across the Union.

[70] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202500038

3 Standards, Schemas, Criteria and Scales

In this chapter, we link the findings of chapter 2 by adopting specific scales to facilitate the certification process of the sector-specific professional trainings. The micro-credentials approach, as presented in D3.2, is mapped to a ECTS credits approach to align the final certification scheme with the CyberSecPro Grant Agreement.

3.1 Factors and Standards

We confirm that the factors and standards remain fit-for-purpose following the WP5 analysis. Therefore, no updates exist compared to D3.2.

3.2 Criteria

We confirm that the criteria remain fit-for-purpose following the WP5 analysis. Therefore, no updates exist compared to D3.2. No updates exist as compared to the deliverable D3.2.

3.3 Scales

3.3.1 European Credit Transfer and Accumulation System (ECTS)[71,72]

The European Credit Transfer and Accumulation System (ECTS) is **a standard used across European higher education institutions to quantify the workload required for academic modules or programmes**. The system helps ensure transparency in the recognition of academic qualifications and facilitates the transfer of credits between higher education institutions.

To calculate the ECTS for an academic module, certain criteria must be considered. Here's a breakdown of how to determine the number of ECTS credits for a module:

1. **Workload (Total Student Effort)**

   ECTS credits are based on the total workload a student needs to complete the module, including both contact hours (direct interaction with teachers) and independent learning (self-study, assignments, exams, etc.).

   - **1 ECTS credit = 25 to 30 hours of total workload**. Therefore, the number of ECTS credits corresponds to the total number of hours a student is expected to invest in the academic module.

2. **Breakdown of Workload Components**

   The total workload may be broken down into different categories:

   - Lectures/Classes/Contact Hours: These are the hours spent in direct instruction, typically face-to-face, online, or hybrid.
   - Practical Work: This includes lab sessions, group work, seminars, workshops, fieldwork, and other activities where students apply theoretical knowledge in practice.
   - Independent Study: This includes time spent reading textbooks, preparing for seminars, writing essays or reports, working on assignments, and studying for exams.

[71] https://op.europa.eu/en/publication-detail/-/publication/9ac30b32-f6af-486e-ba4b-891459942bfd
[72] https://education.ec.europa.eu/education-levels/higher-education/inclusive-and-connected-higher-education/european-credit-transfer-and-accumulation-system

- Assessment Tasks: Time required for preparing and completing assignments, projects, case studies, or exams should also be considered.
- Examinations: Time spent on final exams, mid-term exams, or other evaluative assessments should be included in the total workload.

3. **Types of Learning Activities**

Different types of learning activities contribute differently to the total workload, and this should be considered when estimating the total hours. For example:

- Lecture (1 hour): Might require an additional 1-2 hours of independent study or preparation.
- Seminars/Group Work (1 hour): Could require 2-3 hours of preparation and follow-up work.
- Projects or Practical Work: Typically, 1 hour of practical work could equate to 2-3 hours of student effort depending on the complexity.

4. **Level of Study**

The level of the module (e.g., undergraduate, graduate, doctoral) can also impact how ECTS is calculated, as higher-level courses usually involve more independent study and research.

- Undergraduate courses often have a higher proportion of contact hours.
- Postgraduate courses typically involve more independent study and research, requiring more hours outside of formal instruction.

5. **Considerations for Internationalization and Transfer**
   - Consistency across institutions: ECTS provides a consistent method for credit transfer and recognition across different higher education institutions in Europe. Therefore, while the number of ECTS credits may vary depending on the workload, the methods for calculating these credits remain standardized to ensure mutual recognition.
   - Module Learning Outcomes: In addition to workload, the learning outcomes of the module should align with the expected level of achievement in the ECTS framework. Higher-level modules (e.g., Master's courses) will typically require a deeper level of analysis and critical thinking, contributing to a greater workload and number of credits.
6. **ECTS Credits in Programmes**
   - A full academic year is typically worth 60 ECTS credits, with each semester contributing approximately 30 ECTS credits.
   - A Bachelor's degree generally requires 180 ECTS credits (3 years).
   - A Master's degree generally requires 120 ECTS credits (2 years).

3.3.2 Micro-credentials[73,74,75]

As mentioned in the deliverable D3.2, the micro-credentials are the record of the **learning outcomes**, (i.e., the acquisition of specific skills or competencies) that a learner has acquired following **a small volume of learning**. These learning outcomes will have been assessed against transparent and clearly defined criteria. Learning experiences leading to micro-credentials are designed to provide the learner with specific knowledge, skills and competences that respond to societal, personal, cultural, or labour market needs. Micro-credentials are owned by the learner, can be shared and are portable. They may be standalone or combined into larger credentials. They are underpinned by quality assurance following agreed standards in the relevant sector or area of activity.

[73] https://www.etf.europa.eu/sites/default/files/2023-05/Micro Credential%20Guidelines%20Final%20Delivery.pdf
[74] https://education.ec.europa.eu/education-levels/higher-education/micro-credentials
[75] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(02)

We breakdown the criteria for calculating the micro-credentials for a professional training module, as follows:

1. **Learning Outcomes**

The primary criterion for determining a micro-credential is the learning outcomes that a participant is expected to achieve. Micro-credentials should be based on clear, measurable outcomes that demonstrate the learner's new knowledge, skills, or competencies in a specific field.

- Competency-Based: The focus should be on what the learner is able to do after completing the module (e.g., specific technical skills, problem-solving abilities, leadership qualities, etc.).
- Skills and Knowledge: Identify whether the micro-credential addresses technical, cognitive, or interpersonal skills and how these can be evaluated.

2. **Total Learning Hours (Workload)**

Micro-credentials are often shorter and more focused than ECTS in full academic modules, but they still require an estimation of the total workload the learner will need to complete the module. This can include:

- Contact Hours: Direct instructional time (e.g., lectures, live webinars, workshops).
- Independent Study: Time for reading, research, assignments, and practice.
- Assessments: Time required to complete quizzes, projects, or tests.
- Practice Hours: In some cases, practical or hands-on experience, such as completing a project or simulation.

3. **Level of Complexity or Depth**

Micro-credentials should reflect the level of complexity or depth of the skills and knowledge being acquired. This can be assessed based on:

- Entry-Level: Basic understanding or introductory skills in a particular subject area.
- Intermediate-Level: A deeper, more nuanced understanding or application of concepts.
- Advanced-Level: High-level, specialized expertise or proficiency in complex concepts.

4. **Assessment and Evaluation**

A key factor in awarding a micro-credential is the assessment that confirms the learner's proficiency. There are several types of assessments that may be used:

- Formative Assessments: Ongoing feedback during the training module, such as quizzes, discussions, or assignments, to help learners progress.
- Summative Assessments: A final exam, project, or practical task that evaluates the learner's ability to apply the knowledge gained.
- Competency-Based Evaluation: Rather than just testing knowledge, many micro-credentials assess whether learners can demonstrate specific competencies in real-world scenarios, such as solving a problem or completing a project.
- Certification: To ensure validity, micro-credentials often involve a certification process, confirming that learners meet the established criteria.

5. **Flexibility and Delivery Mode**

Micro-credentials can be delivered in different formats, and this can impact the calculation of the time and effort required:

- Online/Hybrid: If the training is delivered online or in a hybrid format, the learner's ability to work at their own pace can affect the total hours.
- In-person/Instructor-Led: For in-person or live sessions, the total time might be more rigid.

The delivery mode should be factored into the total time and effort the learner needs to invest, with more flexible formats possibly requiring less structured time commitment.

6. **Industry and Stakeholder Recognition**

One important factor in determining the value of a micro-credential may be its recognition within the industry. The micro-credential should align with the needs of the labour market or industry standards.

- Relevance to Job Market: If the training module addresses a key skill or knowledge gap in a particular profession (e.g., cybersecurity, network engineering, etc.), it can help attract professionals seeking to validate their skills.
- Employer Demand: Understanding which competencies are sought by employers can help determine the scope and depth of the micro-credential.

7. **Stackability and Recognition**

A micro-credential should be stackable, meaning that it can be accumulated over time to form part of a larger qualification or learning pathway. Some professional training modules can be combined to create a broader qualification.

- Modular Learning: If multiple micro-credentials are part of a broader professional development pathway (e.g., a certificate in project management made up of several smaller micro-credentials), the learner may accumulate credits over time.
- Badges or Digital Credentials: Many micro-credentials use digital badges to verify completion and allow learners to showcase their new skills on platforms like LinkedIn.

8. **Duration and Intensity**

Professional training modules are typically much shorter than academic ones. Their duration and intensity may vary:

- Short, Self-paced: These micro-credentials may take a few hours to a week (e.g., introductory modules).
- Longer, More Intensive: Some may take several weeks or months to complete, depending on the learning outcomes and complexity.

3.3.3 Micro-credentials to ECTS mapping

Mapping micro-credentials to ECTS is an essential process for ensuring that short, specialized training or certifications align with the broader European higher education framework. This ensures the transferability and recognition of these micro-credentials across institutions and industries, providing learners with a clear understanding of their educational value.

A proposed path to accomplish this mapping is as follows:

1. Define clear learning outcomes that align with the ECTS framework.
2. Estimate the total workload (including lectures, self-study, and assessments) based on the time learners will spend.
3. Align the micro-credentials with the appropriate ECTS level based on the complexity of the subject matter.
4. Ensure that the micro-credential includes valid assessments to verify the learning outcomes.
5. Provide certification or digital badges that clearly indicate the ECTS credits awarded, and the competencies achieved.
6. Make the micro-credential stackable and transferable, allowing learners to use it as part of broader qualifications.

4 CyberSecPro Schema for cybersecurity trainings

4.1 Principles and Standards to be used

No updates exist as compared to the deliverable D3.2.

4.2 Criteria & Scales

4.2.1 Criteria

No updates exist as compared to the deliverable D3.2.

4.2.2 Scales: The Micro-Credentials Case

As mentioned in section 3.3.2 and in the deliverable D3.2, to calculate the volume of the micro-credentials for each professional training module (i.e., course, workshop, seminar, exercise, hackathon) we first need to describe the factors of which the formula is comprised of.

First, the **workload** factor (**F_W**), which equals to the sum of attendance hours plus the study hours (i.e. self-study and assignments preparation). *Second*, the **level** factor (**F_L**), which is either *Basic* or *Advanced* and it corresponds to the training module level. *Third*, the **circle** factor (**F_C**), which stands for n^{th} times of repetition regarding the training module delivery (e.g., $F_c = 1$ if the training module curriculum needs only 1 time (i.e., week) to be offered and $F_c = 12$ if the training module curriculum needs 12 times (i.e., weeks) to be offered. *Forth*, the **assessment** factor (**F_A**), which is *Exercise* or *Exam* or *Project* and it corresponds to the training module assessment type. *Fifth*, the **participation** factor (**F_{PA}**), which is *Online* or *Physical* and corresponds to the trainees type of participation during the training offering. *Sixth*, the **prerequisites** factor (**F_{PQ}**), which is either *Yes* or *No* for the cases that a training module participation needs prior training knowledge of another module.

The CyberSecPro projects proposes Formula 1 to calculate the **micro-credentials (MC) volume**.

$$\boldsymbol{MC} = 0{,}1 \times (F_w + F_L + F_C + F_{PA} + F_{PQ}) \qquad (1)$$

Where:

$$F_w = Attendance\ in\ lectures\ and\ labs + Study, \qquad F_w \in \mathbb{Z}\ \text{hours}$$

$$F_L = \begin{cases} 1, & for\ Basic\ Level\ Course \\ 2, & for\ Advanced\ Level\ Course \end{cases}$$

$$F_c \in [1{,}12], \qquad F_c \in \mathbb{Z}$$

$$F_{PA} = \begin{cases} 1, & when\ Participation\ is\ Online \\ 2, & when\ Participation\ is\ Physical \end{cases}$$

$$F_{PQ} = \begin{cases} 1, & without\ Prerequisites \\ 2, & with\ Prerequisites \end{cases}$$

4.2.3 Scales: The Micro-Credentials to ECTS Mapping Case

As mentioned in section 3.3.1 and as it is widely used from the European higher education institutions (HEIs), the formula to calculate **the ECTS credits for each academic module is as follows**.

$$ECTS\ credits = \frac{Student\ Workload\ (in\ hours)}{25}$$

Despite the fact that CyberSecPro project only offers professional training modules, and, hence, it issues micro-credentials to the trainees, we propose the following formula for mapping the issued micro-

credentials to ECTS credits. It must be noted that the introduced **Formula 2** refers to any CyberSecPro training module type excluding the course type. Regarding the case where the offering module corresponds to a course, we introduce the following **Formula 3**. From Formula 1, it is derived that:

$$ECTS_{training\ modules} = \frac{F_w}{25} \qquad (2)$$

Where:

$$F_w = Attendance\ in\ lectures\ and\ labs + Study, \qquad F_w \in \mathbb{Z}\ \text{hours}$$

From formulas 1 and 2, we introduce Formula 3 as follows.

$$ECTS_{training\ course} = \frac{F_w + F_M}{25} \qquad (3)$$

Where:

$$F_M = Mentoring, \qquad F_M \in \mathbb{Z}\ \text{hours}$$

As previously mentioned, Formula 3 refers only to the course type of professional training, and it introduces a new factor; the **mentoring** factor, which is deeply examined in the literature[76,77,78,79,80,81,82,83,84,85,86]. A course is the most completed knowledge-oriented flavour of a CyberSecPro module and it requires more effort from the trainees, as compared to the other type of module offerings. This effort is required due to the course's repetitive nature (i.e., nine to twelve weeks), as well as its in-depth nature. Therefore, the trainees may require specific assistance, such as mentoring. Mentoring is measured in hours, and it corresponds to personal or small group meetings, online guidance, and email or messages communication. Also, mentoring plays a critical role in professional training courses because it directly enhances the effectiveness, relevance, and sustainability of skills development. Its importance can be explained across several complementary dimensions.

First, mentoring supports the **translation of theoretical knowledge into professional practice**. Professional training courses often introduce complex concepts, frameworks, and methodologies. Mentors help learners contextualise this knowledge within real-world environments, guiding them in applying abstract principles to practical scenarios, decision-making processes, and problem-solving activities. This is particularly important in domains such as cybersecurity, where operational judgement and experience-based reasoning are essential.

Second, mentoring enables **individualised learning and competence development**. Unlike standardised training delivery, mentoring allows for personalised guidance based on the learner's background, role, and learning pace. Mentors can identify skill gaps, reinforce strengths, and adapt

[76] https://link.springer.com/article/10.1186/s12909-024-06357-3
[77] https://www.ncbi.nlm.nih.gov/books/NBK552775/
[78] https://link.springer.com/article/10.1007/s10734-023-01042-8
[79] https://www.mdpi.com/2227-7102/11/10/574
[80] https://epale.ec.europa.eu/sites/default/files/io2_toolkit_wbl_practices_in_europe-en.pdf
[81] https://cor.europa.eu/en/news/mentoring-powerful-tool-tackling-inequality
[82] https://www.skillsforemployment.org/knowledge-product-detail/4911
[83] https://www.cedefop.europa.eu/files/4117_en.pdf
[84] https://www.oecd.org/en/publications/getting-skills-right-future-ready-adult-learning-systems_9789264311756-en.html
[85] https://www.enisa.europa.eu/sites/default/files/publications/ENISA_Report-Addressing_Skills_Shortage_And_Gap_Through_Higher_Education.pdf
[86] https://www.iso.org/standard/52993.html

learning pathways, accordingly, thereby increasing the likelihood that learning outcomes are effectively achieved.

Third, mentoring contributes to the **development of professional behaviours and soft skills**. Beyond technical knowledge, professional competence includes ethical conduct, communication, teamwork, and accountability. Through continuous interaction and role modelling, mentors transmit professional norms and best practices that are difficult to convey through formal instruction alone.

Fourth, mentoring strengthens **learner engagement and retention**. Ongoing mentor support provides motivation, feedback, and reassurance, reducing dropout rates and enhancing commitment to the training programme. Learners are more likely to persist and perform effectively when they have access to structured guidance and constructive feedback.

Fifth, mentoring supports **quality assurance and skills validation**. Mentors can observe learner performance in practical exercises, simulations, or workplace-based activities, providing formative assessments and evidence of competence development. This is particularly relevant for professional training schemes that aim to validate skills and knowledge rather than merely certify course completion.

Sixth, mentoring facilitates **career development and professional integration**. Mentors can offer insights into career pathways, sector-specific expectations, and professional standards, helping learners align their training outcomes with labour market needs. This guidance enhances employability and supports smoother transitions into professional roles.

In summary, mentoring is of great importance in professional training courses because it bridges the gap between learning and practice, it personalises competence development, it reinforces professional standards, and it enhances both training quality and learner outcomes.

4.3 CyberSecPro Schema

A robust cybersecurity certification schema succeeds when **assessment criteria, evaluation methodology, and profiles are tightly aligned**. Misalignment—such as advanced profiles assessed only through basic exams—undermines credibility and workforce trust. Table 9 presents how these three pillars are connected to the certification process.

Table 9. Three pillars of a certification schema

Pillar	**Core Question Answered**
Assessment Criteria	*What competencies must be demonstrated?*
Evaluation Methodology	*How are those competencies verified?*
Profiles	*For which roles and levels is this certification intended?*

Additionally, the ECSF should be noted as the alignment backbone for such a process. As previously mentioned, the ECSF provides a **common European reference model** for cybersecurity roles by defining:

- 12 cybersecurity professional profiles
- Role purpose and responsibilities
- Expected outcomes
- Tasks, skills, and knowledge
- Four proficiency levels (EQF-aligned)

Therefore, certification schemes aligned with ECSF must **derive their internal logic from these definitions**, rather than inventing proprietary role or level taxonomies.

4.3.1 Assessment Criteria

In an ECSF-aligned scheme, assessment criteria are:

- **Mapped directly to ECSF profiles**
  - Each criterion references:
    - ECSF role purpose
    - ECSF tasks and deliverables
    - ECSF-required knowledge and skills
- **Level-specific**
  - Criteria explicitly distinguish between ECSF proficiency levels (e.g., Level 2 vs Level 4)
  - Emphasis shifts from execution → autonomy → strategic responsibility
- **Outcome-oriented**
  - Focus on *what the professional can deliver*, not just what they know
  - Examples:
    - "Perform threat monitoring" (Level 1–2)
    - "Design and oversee SOC operations" (Level 3–4)

What ECSF Prevents

- Arbitrary role naming
- Inflated "expert" certifications without corresponding responsibility
- Knowledge-only certifications claiming professional equivalence

Result:
Assessment criteria become **transparent, comparable, and role-specific across Europe**.

4.3.2 Evaluation Methodology

While ECSF does not prescribe assessment methods, it **constrains methodology by role and level**:

- **Lower proficiency levels**
  - Emphasis on:
    - Structured exams
    - Guided practical exercises
    - Supervised labs
  - Goal: verify foundational capability and correct execution
- **Higher proficiency levels**
  - Emphasis on:
    - Scenario-based assessments
    - Case studies and architectural reviews
    - Decision-making under constraints
  - Goal: verify autonomy, judgment, and accountability
- **Professional validation**

    - For senior ECSF profiles:
        - Experience evidence
        - Peer review or endorsement
        - Continuing professional development (CPD)

- **ECSF Quality Implications**

An ECSF-aligned scheme must demonstrate:

- **Validity**: the method measures ECSF-defined outcomes
- **Proportionality**: assessment rigor matches ECSF level
- **Traceability**: each evaluation component maps back to ECSF skills/tasks

Result:
Evaluation methodology becomes **fit-for-purpose**, avoiding over-testing juniors and under-testing senior professionals.

4.3.3 Profiles

In ECSF-aligned schemes:

- **Profiles are not invented**
    - They correspond directly to ECSF roles such as:
        - Incident Responder
        - Digital Forensics Investigator
        - Cybersecurity Architect
        - Cybersecurity Risk Manager
- **Profiles include explicit boundaries**
    - What the role is responsible for
    - What it is *not* responsible for
    - Interaction with other ECSF roles
- **Profiles are level-aware**
    - The same ECSF role may exist at multiple proficiency levels
    - Certification titles must reflect this clearly
- **Labor-Market Value**

Because ECSF profiles are shared across:

- Employers
- Training providers
- Regulators
- Public-sector frameworks

…certifications aligned with ECSF provide **immediate interpretability and trust**.

Result:
A certification signals *exactly* what role and level a professional can perform—without ambiguity.

4.3.4 CyberSecPro Certificates Design

A **well-designed certificate**[87,88] performs functions that extend substantially beyond the mere confirmation of attendance. It operates as a symbolic and visual indicator of the standards, rigor, and institutional quality underpinning a workshop or training program. Research in perception and evaluation suggests that individuals frequently infer overall quality from presentation cues. Accordingly, a certificate that is carefully structured, aesthetically balanced, and professionally formatted implicitly communicates those comparable levels of diligence and organization characterized the educational experience itself. Conversely, a poorly designed document may inadvertently diminish the perceived legitimacy of an otherwise high-quality workshop by conveying informality or insufficient institutional seriousness.

In addition, a professionally designed certificate contributes to the enhancement of perceived value. Upon completion of a learning experience, participants often seek a tangible representation of their intellectual and temporal investment. The certificate fulfills this symbolic function. When it conveys formality, coherence, and visual refinement, it reinforces the perception that the completed program was substantive and worthwhile. Such symbolic reinforcement influences post-experience evaluations, shaping both memory consolidation and subsequent word-of-mouth communication.

The issuance of a certificate also carries important psychological and affective implications. Formal recognition validates individual effort and achievement, thereby fostering a sense of accomplishment and professional identity. A thoughtfully designed certificate amplifies this effect by enhancing the symbolic weight of the recognition. Recipients are more likely to retain, display, or disseminate a credential that reflects institutional credibility and aesthetic quality. This emotional engagement can strengthen long-term affiliation with the issuing organization and deepen the perceived significance of the learning experience.

From a strategic perspective, certificates may also function as instruments of reputational extension. Participants frequently share their achievements on professional and social networking platforms such as LinkedIn and Instagram. When certificates incorporate coherent branding and professional design standards, such public displays contribute to organic visibility and serve as forms of social validation. In this manner, the certificate operates not only as a record of completion but also as a mechanism of indirect institutional promotion.

Furthermore, a well-designed certificate reinforces organizational identity. Each point of interaction between participants and an institution contributes cumulatively to brand perception. Visual inconsistency between instructional materials and certification documents may undermine coherence and weaken perceived professionalism. In contrast, alignment in typography, color systems, and structural design strengthens brand continuity, thereby fostering trust and institutional recognition over time.

Within professional contexts, certificates may also play a practical role in career development. Participants frequently append them to employment applications, professional profiles, or portfolios. When certificates clearly articulate essential information—such as program title, completion date, duration, and instructor credentials—they facilitate external evaluation of the credential's relevance.

---

87 https://share.ansi.org/wc/Shared%20Documents/Workcred-Reports/The-Role-of-Certificates-in-Signifying-Knowledge-and-Skills-Attainment.pdf

88 https://www.oecd.org/en/publications/the-theory-and-practice-of-upper-secondary-certification_b3fea5ba-en/full-report/towards-principles-and-a-matrix-for-the-design-of-upper-secondary-certificates_650dfb07.html

Structural clarity and visual organization enhance interpretability and credibility, whereas ambiguity or poor formatting may reduce their persuasive efficacy.

Ultimately, the design of a certificate communicates institutional respect for participants' time, commitment, and achievement. By presenting recognition in a deliberate and professional manner, the issuing body affirms the value of the learner's effort. As certificates often constitute the final formal interaction within a workshop experience, their quality significantly shapes enduring impressions and influences future engagement decisions.

In the context of the CyberSecPro project, the design materials regarding the certificates are as follows:

1. Code of the module and module(s) titles(s)
2. Trainee name and surname
3. Organisation(s) included
4. Logos
5. Micro-credentials and/or the number of ECTS credits
6. Location, region, and country
7. Signatures
8. Number of hours (# h)
9. Date/s
10. QR / Website of the CyberSecPro project
11. Type of certificate: "Certificate of Attendance" / "Certificate of Completion".
12. Level of the module: basic / advanced
13. Type of module: Online / Physical

A template example of a CyberSecPro certificate is presented in Annex A.

Electronic Badges on Completing a CyberSecPro Training

An **electronic badge (e-badge)**[89,90,91], commonly referred to as a digital badge, represents a verifiable digital credential that signifies the attainment of a defined skill, competency, or program outcome. In contrast to traditional certificates, which typically exist as static printed documents or non-interactive digital files, e-badges incorporate embedded metadata that documents the conditions under which the credential was awarded. Such metadata commonly includes the issuing organization, the criteria for achievement, the date of issuance, and, in certain instances, evidence of the recipient's work or performance.

Although visually presented as a badge or emblem, an e-badge is fundamentally a data-rich credential. The embedded, machine-readable information enables independent verification of authenticity and ensures portability across digital platforms. The conceptual development of interoperable badge systems

[89] https://doi.org/10.1186/s41239-019-0175-9
[90] https://www.mdpi.com/2076-3417/12/1/220
[91] https://doi.org/10.1007/s11528-017-0168-2

was significantly influenced by initiatives such as the Open Badges standard introduced by the Mozilla Foundation, which established a framework for cross-platform validation and recognition.

E-badges are increasingly utilized across higher education, professional development, corporate training, and online learning environments. They are frequently administered through specialized credentialing platforms such as Credly and Accredible, which maintain secure records and verification infrastructures. Recipients may display these credentials on professional networking platforms, including LinkedIn, as well as on personal websites and digital portfolios, thereby facilitating transparent validation of competencies.

From an educational standpoint, e-badges align closely with competency-based and outcomes-oriented pedagogical frameworks. They enable granular recognition of discrete skills and support the development of micro-credentialing systems and modular learning pathways. By explicitly articulating assessment standards and achievement criteria, e-badges enhance transparency in credentialing practices and provide stakeholders—including employers, academic institutions, and professional bodies—with clearer evidence of demonstrated capabilities.

In summary, an e-badge constitutes a portable, authenticated, and metadata-enriched digital credential designed to document and communicate verified achievements within contemporary educational and professional ecosystems.

4.3.5 The Certification Schema

A summarisation of the core elements of the CyberSecPro sector-specific cybersecurity professional training certification scheme is as follows:

- **Scope:** To offer practical and theoretical trainings in sector-specific cybersecurity areas.
- **Target Audience**: Individuals and professionals from sector-specific fields.
- **Structure:** 72 sector-specific training modules (i.e., courses, workshops, seminars, hackathons, exercises). 14 of these modules (i.e., the courses type) comprise a concrete offering of **60 ECTS credits and may be considered as the core of an Executive Masters Programme**.
- **Assessment principles:** Trainees have to register and attend the lectures/hands-on trainings. During this attendance and for the completion of the process, the trainees are required to submit exercises or projects or to give exams, as the assessment requirements for each module.
- **Applicable scales:** Each module offers micro-credentials to the trainees. The 14 modules (i.e., the courses type) also offer ECTS credits.

Table 10 describes a full breakdown of the 14 the CyberSecPro sector-specific modules which comprise the project's certification schema by aligning their design, content, and outcomes, while Table 11 illustrates how these modules line up to the ECSF backbone and the European Skills, Competences, and Occupations (ESCO)[92,93] classification.

[92] https://esco.ec.europa.eu/en
[93] https://www.enisa.europa.eu/sites/default/files/2024-12/esco-ecsf-crosswalk.pdf

Table 10. The CyberSecPro certification schema

CSP Module Name	Provider	Microcredentials Calculation									
		Workload (in hours)			Level	Cycle	Assessment type	Participation type	Prerequisites	TOTAL Microcredentials	ECTS credits
		Lectures Attendance	Hands-on / Self-study/ Practical	Mentoring	Basic / Advanced	N^{th} time of repetition	Exercise / Exam / Project	Online / Physical	Yes / No		
CSP001_C_E: Cybersecurity Essentials and Management for Energy Sector	LAU_UMA_SGI_PDMFC_ TRUSTILLIO_TALTECH	33	55	12	Basic	11	Project	Online	Yes	11	4
CSP001_C_M: Cybersecurity Essentials and Management for Maritime	UPRC_LAU	36	50	14	Basic	12	Project	Physical	No	11	4
CSP003_C_H: Cybersecurity Risk Management and Governance in the Healthcare sector	APIRO_UPRC	18	40	42	Advanced	9	Project	Physical	No	8	4
CSP004_C_E: Network Protection for Energy Control Systems - Part I *	UMA_AIT	30	60	10	Advanced	10	Project	Online	Yes	11	4
CSP004_C_E: Network Protection for Energy Control Systems - Part II *	UMA_AIT	30	60	10	Advanced	10	Project	Online	Yes	11	4
CSP004_C_E: Network Security for Energy	TUBS	24	50	26	Basic	12	Exercise	Physical	No	9	4
CSP006_C_E: Cyber Threat Intelligence in the Energy Network	FCT	36	52	12	Advanced	12	Exam & Project	Physical	Yes	12	4
CSP007_C_E: Cybersecurity in Emerging Technologies for Energy	FCT_UNINOVA_LAU	24	64	12	Advanced	12	Exam & Project	Physical	Yes	12	4
CSP008_C_H: Advanced Infrastructure Security for Health	PDM	30	50	20	Advanced	10	Project	Physical	Yes	10	4
CSP008_C_E: Critical Energy Infrastructure Security	FCT_UNINOVA_PDMFC	24	64	12	Advanced	12	Exam & Project	Physical	Yes	12	4
CSP008_C_M: Critical Infrastructure Security for Maritime	C2B	30	50	20	Basic	10	Project	Physical	No	10	4
											44
MOOC on Human Factors of Cybersecurity +	TalTech	30	80	40	Advanced	10	Exam	Online	Yes	11	6
MOOC - CyberSecPro: Cybersecurity Fundamentals +	PDM	37	50	38	Basic	10	Project	Online	No	10	5
MOOC - From Zero to Hero: A Complete Cybersecurity Toolkit +	PDM	40	50	35	Advanced	10	Exercises	Online	Yes	10	5
											16
										TOTAL ECTS offered	**60**

***** The syllabi and the descriptions of the modules CSP004_C_E Part I and Part II are presented in Annex B.

+ The descriptions and syllabi of the MOOCs are presented in the deliverables D4.2 and D4.5.

Table 11. The certification schema alignment to the ECSF profiles and the ESCO occupations

CSP Module Name	e-Competencies: Level Specific	ECSF Role Profiles	ESCO Occupations
CSP001_C_E: Cybersecurity Essentials and Management for Energy Sector	A.7. Technology Trend Monitoring (Level 4) D.1. Information Security Strategy Development (Level 5) E.3. Risk Management (Level 4) E.8. Information Security Management (Level 4) E.9. IS-Governance (Level 5)	**Chief Information Security Officer (CISO)**	Chief ICT Security Officer
CSP001_C_M: Cybersecurity Essentials and Management for Maritime	A.1. Information Systems and Business Strategy Alignment (Level 4) A.7. Technology Trend Monitoring (Level 4) B.3. Testing (Level 4) B.5. Documentation Production (Level 3) D.1. Information Security Strategy Development (Level 4-5) E.3. Risk Management (Level 4) E.5. Process Improvement (Level 3) E.6 ICT Quality Management (Level 4) E.7. Business Change Management (Level 4) E.8. Information Security Management (Level 3-4) E.9. IS-Governance (Level 4-5)	**Chief Information Security Officer (CISO) // Cyber Legal, Policy & Compliance Officer // Cybersecurity Auditor // Cybersecurity Risk Manager**	Chief ICT Security Officer // Data Protection Officer // IT Auditor & ICT Auditor Manager // Cybersecurity Risk Manager
CSP003_C_H: Cybersecurity Risk Management and Governance in the Healthcare sector	A.5. Architecture Design (Level 5) A.6. Application Design (Level 3) B.1. Application Development (Level 3) B.2. Component Integration (Level 4) B.3. Testing (Level 3-4) B.4. Solution Deployment (Level 2) B.5. Documentation Production (Level 3) B.6. ICT Systems Engineering (Level 4)	**Cybersecurity Architect // Penetration Tester**	ICT System Architect & System Architect & Cloud Architect & Network Architect // Ethical Hacker
CSP004_C_E: Network Protection for Energy Control Systems - Part I	A.7. Technology Trend Monitoring (Level 3-5) A.9. Innovating (Level 5) B.2. Component Integration (Level 2-4) B.3. Testing (Level 3-4) B.5. Documentation Production (Level 3) C.4. Problem Management (Level 3-4) D.7. Data Science and Analytics (Level 4) D.10. Information and Knowledge Management (Level 3) E.3. Risk Management (Level 4) E.6 ICT Quality Management (Level 4)	**Cyber Incident Responder // Cyber Threat Intelligence Specialist // Cybersecurity Architect // Cybersecurity Auditor // Cybersecurity Researcher // Penetration Tester**	Cyber incident responder // Intelligence officer // ICT System Architect & System Architect & Cloud Architect & Network Architect // IT Auditor & ICT Auditor Manager // Research engineer // Ethical Hacker
CSP004_C_E: Network Protection for Energy Control Systems - Part II	A.7. Technology Trend Monitoring (Level 3-5) A.9. Innovating (Level 5) B.2. Component Integration (Level 2-4) B.3. Testing (Level 3-4) B.5. Documentation Production (Level 3) C.4. Problem Management (Level 3-4) D.7. Data Science and Analytics (Level 4) D.10. Information and Knowledge Management (Level 3) E.3. Risk Management (Level 4) E.6 ICT Quality Management (Level 4)	**Cyber Incident Responder // Cyber Threat Intelligence Specialist // Cybersecurity Architect // Cybersecurity Auditor // Cybersecurity Researcher // Penetration Tester**	Cyber incident responder // Intelligence officer // ICT System Architect & System Architect & Cloud Architect & Network Architect // IT Auditor & ICT Auditor Manager // Research engineer // Ethical Hacker
CSP004_C_E: Network Security for Energy	A.5. Architecture Design (Level 3) A.6. Application Design (Level 3) A.7. Technology Trend Monitoring (Level 3)	**Cyber Incident Responder // Cyber Threat Intelligence Specialist // Cybersecurity Implementer // Cybersecurity Risk Manager**	Cyber incident responder // Intelligence officer // Embedded System Security Engineer & ICT Security

	B.1. Application Development (Level 3) B.2. Component Integration (Level 2) B.3. Testing (Level 3) B.5. Documentation Production (Level 3) B.6. ICT Systems Engineering (Level 4) C.4. Problem Management (Level 4) D.7. Data Science and Analytics (Level 4) D.10. Information and Knowledge Management (Level 4) E.3. Risk Management (Level 4) E.4. Relationship Management (Level 3) E.5. Process Improvement (Level 3) E.7. Business Change Management (Level 4) E.8. Information Security Management (Level 4) E.9. IS-Governance (Level 4)		Administrator & ICT Security Technician // Cybersecurity Risk Manager
CSP006_C_E: Cyber Threat Intelligence in the Energy Network	A.7. Technology Trend Monitoring (Level 3-5) A.9. Innovating (Level 5) B.3. Testing (Level 4) B.5. Documentation Production (Level 3) C.4. Problem Management (Level 3) D.7. Data Science and Analytics (Level 4) D.10. Information and Knowledge Management (Level 3-4) E.3. Risk Management (Level 3) E.4. Relationship Management (Level 3) E.8. Information Security Management (Level 4)	**Cyber Threat Intelligence Specialist // Cybersecurity Researcher // Digital Forensics Investigator**	Intelligence officer // Research engineer // Digital Forensics Expert
CSP007_C_E: Cybersecurity in Emerging Technologies for Energy	A.7. Technology Trend Monitoring (Level 3-5) A.9. Innovating (Level 5) B.3. Testing (Level 4) B.5. Documentation Production (Level 3) C.4. Problem Management (Level 3) D.7. Data Science and Analytics (Level 4) D.10. Information and Knowledge Management (Level 3-4) E.3. Risk Management (Level 3) E.4. Relationship Management (Level 3) E.8. Information Security Management (Level 4)	**Cyber Threat Intelligence Specialist // Cybersecurity Researcher // Digital Forensics Investigator**	Intelligence officer // Research engineer // Digital Forensics Expert
CSP008_C_H: Advanced Infrastructure Security for Health	A.7. Technology Trend Monitoring (Level 3-5) A.9. Innovating (Level 5) B.3. Testing (Level 4) B.5. Documentation Production (Level 3) C.4. Problem Management (Level 3) D.7. Data Science and Analytics (Level 4) D.10. Information and Knowledge Management (Level 3-4) E.3. Risk Management (Level 3) E.4. Relationship Management (Level 3) E.8. Information Security Management (Level 4)	**Cyber Threat Intelligence Specialist // Cybersecurity Researcher // Digital Forensics Investigator**	Intelligence officer // Research engineer // Digital Forensics Expert
CSP008_C_E: Critical Energy Infrastructure Security	A.7. Technology Trend Monitoring (Level 3-5) A.9. Innovating (Level 5) B.3. Testing (Level 4) B.5. Documentation Production (Level 3) C.4. Problem Management (Level 3) D.7. Data Science and Analytics (Level 4) D.10. Information and Knowledge Management (Level 3-4) E.3. Risk Management (Level 3)	**Cyber Incident Responder // Cybersecurity Risk Manager // Cyber Legal, Policy & Compliance Officer**	Cyber incident responder // Cybersecurity Risk Manager // Data Protection Officer

	E.4. Relationship Management (Level 3) E.8. Information Security Management (Level 4)		
CSP008_C_M: Critical Infrastructure Security for Maritime	A.1. Information Systems and Business Strategy Alignment (Level 4) A.7. Technology Trend Monitoring (Level 3) B.2. Component Integration (Level 2) B.3. Testing (Level 3) B.5. Documentation Production (Level 3) C.4. Problem Management (Level 4) D.1. Information Security Strategy Development (Level 4) E.3. Risk Management (Level 4) E.5. Process Improvement (Level 3) E.7. Business Change Management (Level 4) E.8. Information Security Management (Level 3) E.9. IS-Governance (Level 4)	**Cyber Incident Responder // Cybersecurity Risk Manager // Cyber Legal, Policy & Compliance Officer**	Cyber Incident Responder // Cybersecurity Risk Manager // Director of Compliance and Information Security & Data Protection Officer
MOOC on Human Factors of Cybersecurity	A.1. Information Systems and Business Strategy Alignment (Level 4) A.5. Architecture Design (Level 3) A.6. Application Design (Level 3) A.7. Technology Trend Monitoring (Level 4-5) A.9. Innovating (Level 5) B.1. Application Development (Level 3) B.3. Testing (Level 3) B.6. ICT Systems Engineering (Level 4) C.4. Problem Management (Level 3) D.1. Information Security Strategy Development (Level 4-5) D.3. Education and Training Provision (Level 3) D.7. Data Science and Analytics (Level 4) D.9. Personnel Development (Level 3) D.10. Information and Knowledge Management (Level 3) E.3. Risk Management (Level 4) E.5. Process Improvement (Level 3) E.7. Business Change Management (Level 4) E.8. Information Security Management (Level 3-4) E.9. IS-Governance (Level 4-5)	**Chief Information Security Officer (CISO) // Cyber Legal, Policy & Compliance Officer // Cybersecurity Educator // Cybersecurity Implementer // Cybersecurity Researcher // Cybersecurity Risk Manager**	Chief ICT security officer // Director of Compliance and Information Security & Data Protection Officer // Higher education lecturer // Embedded system security engineer // Research engineer // Cybersecurity Risk Manager
MOOC - CyberSecPro: Cybersecurity Fundamentals	A.7. Technology Trend Monitoring (Level 4) D.1. Information Security Strategy Development (Level 5) E.3. Risk Management (Level 4) E.5. Process Improvement (Level 3) E.7. Business Change Management (Level 4) E.8. Information Security Management (Level 4) E.9. IS-Governance (Level 4-5)	**Chief Information Security Officer (CISO) // Cybersecurity Risk Manager**	Chief ICT security officer // Cybersecurity Risk Manager
MOOC - From Zero to Hero: A Complete Cybersecurity Toolkit	A.7. Technology Trend Monitoring (Level 3) B.2. Component Integration (Level 4) B.3. Testing (Level 4) B.4. Solution Deployment (Level 2) B.5. Documentation Production (Level 3) E.3. Risk Management (Level 3-4)	**Digital Forensics Investigator // Penetration Tester**	Digital Forensics Expert // Ethical Hacker

5 Conclusion

In conclusion of this deliverable, the CyberSecPro project provides a structured and comprehensive response to the persistent fragmentation of professional cybersecurity training and certification across Europe. By defining a unified, modular certification schema subject to recognition by a higher-level authority, the project directly addresses the lack of interoperability, quality assurance, and mutual recognition that currently characterises sector-specific cybersecurity programmes. The explicit alignment with the ECSF profiles and competences ensures that the proposed training pathways are grounded in a common European skills language, facilitating clearer understanding of professional roles and capabilities among training providers, employers, and learners.

Moreover, the integration of mathematical mappings between micro-credentials and ECTS credits represents a significant step toward standardisation and transparency, enabling comparability with existing academic and professional qualification frameworks. The balanced combination of theoretical instruction and hands-on training supports the development of both foundational knowledge and practical skills required to meet evolving sectoral cybersecurity challenges. Collectively, these elements enhance professional mobility, support career progression, and contribute to the long-term objective of strengthening cybersecurity maturity and workforce resilience across Europe’s digitalised economic sectors.

Annex A: CyberSecPro certificate example

Annex B: Syllabi and Descriptions of the CSP004_C_E Part I and Part II

CSP004_C_E: Network Protection for Energy Control Systems – Part I

Description of Training Module

CPS004_C_E consists of an intensive course, the objective of which is to reinforce security knowledge but from a practical and advanced point of view. Therefore, the module is designed for engineers and IT/OT administrators in charge of managing control networks, and energy professionals with some knowledge of cybersecurity, including among others human operators, managers and directives, energy suppliers, and employees in general of the corporate network. Also, the course can also be taken by students of industrial engineering or computer sciences, researchers, and educators in the field of energy with some knowledge of cybersecurity.

Code *Code format: CSP001_x where x is the training of offering type (see below)*	**CSP004_C_E (Part I)**
Module Title *The title of the training module*	**Network Protection for Energy Control Systems – Part I**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	○ Network Security Management for Energy Control Systems ○ Secure Management of Energy Control Networks and Substations. ○ Energy Control Network Threat Prevention
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Course (C)

Level *Training level: B (Basic), A (Advanced)*	Advanced (A)
Module overview *High-level module overview*	This course aims to provide a clear vision and understanding of current needs, especially those related to the secure deployment of energy control networks and access to their data. The idea is then to show and provide the minimum tools to not only protect communication channels and hosts, but also to give guarantees of "defense in depth" (only at communication level).
Module description *Indicates the main purpose and description of the module.*	The proposal of this course is to provide a clear understanding of the threats in power control networks to subsequently understand the main security weaknesses of TCP/IP protocols and their impact on critical communication networks. To this end, we will also study the security issues of industrial communication protocols and the implications they have on the implementation of TCP/IP protocols such as telnet or File Transfer Protocol (FTP). From this study, we will proceed to analyze the security protocols of the TCP/IP stack and their guarantees for providing secure industrial communication channels, as well as all those perimeter defenses, considering intrusion detection systems, monitoring systems and firewalls (at host level).

Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, learners will have gained the following: **Knowledge:** ● Knowledge of the most common vulnerabilities and threats in specific network systems and their associated protocols – not only in terms of TCP/IP protocols but also those applied in industrial communication networks. ● Knowledge of the most relevant security protocols such as Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) or IPSec, and their importance for the protection of systems and communication networks. ● Knowledge of the most relevant security mechanisms such as IDS/IPS to protect network perimeters and access to private domains, such as corporate networks ● Knowledge of the most relevant security mechanisms to protect the end points of a communication, considering, for example, firewalls. **Skills:** ● Analyse communication scenarios deployed in energy substations or control networks, and identify possible misconfigurations or vulnerabilities that could lead to security risks or threats. ● Configure systems following basic security principles (e.g., user control, port control, etc.). ● Identify and apply those security elements or mechanisms that contribute to improving the security of a communication system. **Competencies:** ● Know how to identify possible misconfigurations or errors that may lead to significant security risks with a serious impact the energy sector. ● Lead the configuration and deployments of secure communication systems for specific energy communication scenarios. ● Take own criteria under critical thinking to identify and apply existing security technologies, mechanisms and protocols to protect the communications of the charging stations and related infrastructures.
Main topics and content list *A list of main topics and key content*	● Introduction to Energy Control Network Protection ● Common Security Weaknesses and Attacks in Energy Control Networks ● Essential Protection for Energy Control Networks ● Advanced Protection for Energy Control Networks
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessment**: through an evaluation test at the end of the course, in addition to performing some practical actions and tasks addressing case studies and practical activities, which should be reported. The idea is that learners will have the opportunity to reflect, analyze and implement specific activities (e.g. analysis of network traffic traces, configurations with errors, etc.), taking into account the application scenario and its level of criticality.
Training Provider	University of Malaga (UMA) and AIT

Name(s) of training providers.	
Contact *Name(s) of the main contact person and their email address.*	Dr. Cristina Alcaraz, University of Malaga, Spain, alcaraz@uma.es Dr. Abdelkader Shaaban, AIT, Austrian Institute of Technology, abdelkader.shaaban@ait.ac.at
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	About 2 weeks, 20 hours for teaching. But the course probably is extended depending on the practical activities.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual, or both. Any information related to the physical location or URL link about the training module, it will be posted on the DCM platform.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security* *KA6 – Privacy and Data Protection* *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	Mainly: ○ KA5 – Network and Communication Security Nonetheless, minor content matches with other including: ○ KA7 – Cybersecurity Threat Management ○ KA9 – Penetration Testing.

Pre-requisites	Basic knowledge of IT, cybersecurity essentials (related to CSP Module 1), and experience with operating systems, network configurations and communication protocols.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	○ ECSF Profile 5: Cybersecurity architect ○ ECSF Profile 12: Penetration tester
Tools to be used *A list of tools that will be used for the operation of this training module.*	GNS3 Client and VM, Kali Linux, Virtualbox, Arpspoof, Bettercap, Wireshark, CloudShark, Hping3, xarp, Arpwatch, Suricata, Snort, Snort Analyzer, Raspberrypi Linux Image, pyModbusTCP, ufw, OpenVAS, Nmap, Nmap-vulners, IPtables, nftables, iPerf3, Scapy, Hydra, Zenmap, Etherape, legion, Ettercap, Vsftpd (ftp client-server), telnet (client-server), fping, ping, ss, OpenVPN/Wireguard, Metasploitable2 VM, Snorpy, the online CVSS 3.0/3.1 calculator, other open-source VPN tools for testing, among others.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	○ Spoken: English ○ Language for the material and the assessment/evaluation: English
ECTS *If applicable, the number of ECTS.*	4
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.
Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

Adapted Syllabus (Part I)

Main topics	Suggested Content
Topic-1: Introduction to Energy Control Network Protection	• Introduce the application scenario (networks, components, protocols) and its scope. • Motive the problem by exposing the main security challenges of power control systems when the new information technologies (mainly with access to the Internet and wireless communication) arise within the operational ecosystems (e.g., cloud/edge computing, IIoT, remote control, blockchain). • Classify threats in energy control networks and real cases (e.g., due to supply chain). To do so, specific repositories such as MITRE ATT&CK (for Industrial Control Systems – specifically looking at those related to energy) and taxonomies will be considered and explored by students. • Case studies and analysis.
Topic-2: Common Security Weaknesses and Attacks in Energy Control Networks	• Highlight the main security weaknesses of the control networks, and particularly of their communication protocols such as ModbusTCP and its lack of security for confidentiality. • Highlight the main security weaknesses of some TCP/IP communication protocols such as HTTP, FTP, Telnet, TCP, UDP. The idea is to show the main weaknesses if industrial communication protocols are applied together with unsecure TCP/IP communication protocols. • List a few typical offensive tools against confidentiality, integrity, and availability, and practical exercises to understand the weaknesses mentioned in the previous point.

CSP004_C_E: Network Protection for Energy Control Systems – Part II

Description of Training Module

CPS004_C_E consists of an intensive course, the objective of which is to reinforce security knowledge but from a practical and advanced point of view. Therefore, the module is designed for engineers and IT/OT administrators in charge of managing control networks, and energy professionals with some knowledge of cybersecurity, including among others human operators, managers and directives, energy suppliers, and employees in general of the corporate network. Also, the course can also be taken by students of industrial engineering or computer sciences, researchers, and educators in the field of energy with some knowledge of cybersecurity.

Code *Code format: CSP001 x where x is the training of offering type (see below)*	**CSP004_C_E (Part II)**
Module Title *The title of the training module*	**Network Protection for Energy Control Systems – Part II**
Alternative Title(s) *Used alternative titles for the same module by many institutes and training providers*	○ Network Security Management for Energy Control Systems ○ Secure Management of Energy Control Networks and Substations. ○ Energy Control Network Threat Prevention
Training offering type *Indicates the module type based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other, please specify the specific type.*	Course (C)
Level *Training level: B (Basic), A (Advanced)*	Advanced (A)
Module overview *High-level module overview*	This course aims to provide a clear vision and understanding of current needs, especially those related to the secure deployment of energy control networks and access to their data. The idea is then to show and provide the minimum tools to not only protect communication channels and hosts, but also to give guarantees of "defense in depth" (only at communication level).

Module description *Indicates the main purpose and description of the module.*	The proposal of this course is to provide a clear understanding of the threats in power control networks to subsequently understand the main security weaknesses of TCP/IP protocols and their impact on critical communication networks. To this end, we will also study the security issues of industrial communication protocols and the implications they have on the implementation of TCP/IP protocols such as telnet or File Transfer Protocol (FTP). From this study, we will proceed to analyze the security protocols of the TCP/IP stack and their guarantees for providing secure industrial communication channels, as well as all those perimeter defenses, considering intrusion detection systems, monitoring systems and firewalls (at host level).
Learning outcomes and targets *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module*	By the end of the training, learners will have gained the following: **Knowledge:** ● Knowledge of the most common vulnerabilities and threats in specific network systems and their associated protocols – not only in terms of TCP/IP protocols but also those applied in industrial communication networks. ● Knowledge of the most relevant security protocols such as Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) or IPSec, and their importance for the protection of systems and communication networks. ● Knowledge of the most relevant security mechanisms such as IDS/IPS to protect network perimeters and access to private domains, such as corporate networks ● Knowledge of the most relevant security mechanisms to protect the end points of a communication, considering, for example, firewalls. **Skills:** ● Analyse communication scenarios deployed in energy substations or control networks, and identify possible misconfigurations or vulnerabilities that could lead to security risks or threats. ● Configure systems following basic security principles (e.g., user control, port control, etc.). ● Identify and apply those security elements or mechanisms that contribute to improving the security of a communication system. **Competencies:** ● Know how to identify possible misconfigurations or errors that may lead to significant security risks with a serious impact the energy sector. ● Lead the configuration and deployments of secure communication systems for specific energy communication scenarios. ● Take own criteria under critical thinking to identify and apply existing security technologies, mechanisms and protocols to protect the communications of the charging stations and related infrastructures.
Main topics and content list *A list of main topics and key content*	● Introduction to Energy Control Network Protection ● Common Security Weaknesses and Attacks in Energy Control Networks ● Essential Protection for Energy Control Networks

	• Advanced Protection for Energy Control Networks
Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes*	**Knowledge-based assessment**: through an evaluation test at the end of the course, in addition to performing some practical actions and tasks addressing case studies and practical activities, which should be reported. The idea is that learners will have the opportunity to reflect, analyze and implement specific activities (e.g. analysis of network traffic traces, configurations with errors, etc.), taking into account the application scenario and its level of criticality.
Training Provider *Name(s) of training providers.*	University of Malaga (UMA) and AIT
Contact *Name(s) of the main contact person and their email address.*	Dr. Cristina Alcaraz, University of Malaga, Spain, alcaraz@uma.es Dr. Abdelkader Shaaban, AIT, Austrian Institute of Technology, abdelkader.shaaban@ait.ac.at
Dates offered *Indicates the semester / specific dates for the schedule of the trainings, as well as periodicity (e.g., even after the end of the CSP programme).*	Refer and check online CyberSecPro DCM System for current information.
Duration *Duration of the training.*	About 2 weeks, 20 hours for teaching. But the course probably is extended depending on the practical activities.
Training method and provision *Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.*	Physical, virtual, or both. Any information related to the physical location or URL link about the training module, it will be posted on the DCM platform.
Knowledge area(s) *Mapping to the 10 selected CSP knowledge areas.* *KA1 – Cybersecurity Management* *KA2 – Human Aspects of Cybersecurity* *KA3 – Cybersecurity Risk Management* *KA4 – Cybersecurity Policy, Process, and Compliance* *KA5 – Network and Communication Security*	Mainly: ○ KA5 – Network and Communication Security Nonetheless, minor content matches with other including: ○ KA7 – Cybersecurity Threat Management ○ KA9 – Penetration Testing.

KA6 – Privacy and Data Protection *KA7 – Cybersecurity Threat Management* *KA8 – Cybersecurity Tools and Technologies* *KA9 – Penetration Testing* *KA10 – Cyber Incident Response*	
Pre-requisites	Basic knowledge of IT, cybersecurity essentials (related to CSP Module 1), and experience with operating systems, network configurations and communication protocols.
Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles needs this module.*	○ ECSF Profile 5: Cybersecurity architect ○ ECSF Profile 12: Penetration tester
Tools to be used *A list of tools that will be used for the operation of this training module.*	GNS3 Client and VM, Kali Linux, Virtualbox, Arpspoof, Bettercap, Wireshark, CloudShark, Hping3, xarp, Arpwatch, Suricata, Snort, Snort Analyzer, Raspberrypi Linux Image, pyModbusTCP, ufw, OpenVAS, Nmap, Nmap-vulners, IPtables, nftables, iPerf3, Scapy, Hydra, Zenmap, Etherape, legion, Ettercap, Vsftpd (ftp client-server), telnet (client-server), fping, ping, ss, OpenVPN/Wireguard, Metasploitable2 VM, Snorpy, the online CVSS 3.0/3.1 calculator, other open-source VPN tools for testing, among others.
Language *Indicates the spoken language and the language for the material and the assessment/evaluation.*	○ Spoken: English ○ Language for the material and the assessment/evaluation: English
ECTS *If applicable, the number of ECTS.*	4
Certificate of Attendance (CoA) *Indicates Yes or No (even in case of partial attendance)*	No
Module enrolment dates *Indicates the enrolment dates for the operation of this training module.*	Refer and check online CyberSecPro DCM System for current information.

Other important dates *If applicable, any other important dates for this module (such as exam dates, tutoring dates, online dates, face-to-face dates). More information will be provided in the module description.*	Refer and check online CyberSecPro DCM System for current information.

Adapted Syllabus (Part II)

Main topics	Suggested Content
Topic-3: Essential Protection for Energy Control Networks	• Provide an overview of the main TCP/IP security protocols such as TLS, IPSec and SSH, and how they can be adapted in operational networks. • Explore security measures for endpoints like Human-Machine Interfaces (HMIs), analyzing specific vulnerabilities (e.g., unsecured open ports and CVEs), as well as configuring firewall rules at the operating system level (Linux) to prevent possible intrusions. • Practical Exercises.
Topic-4: Advanced Protection for Energy Control Networks	• Introduce intrusion detection mechanisms and techniques and then specify detection at the network level where communication is based on industrial communication protocols such as ModbusTCP. • Provide advanced monitoring mechanisms that controls the security management in energy control networks, as well as the logs that management endpoints such as IT and OT devices. • Practical Exercises.