Project No. 101083594
Call: DIGITAL-2021-SKILLS-01

Project start: 2022-12-01
Project duration: 36 months

CyberSecPro

D4.2

Reports and Training Material on the Cybersecurity Principles and Management Training Modules

Document Identification	
Due date	2024-02-27
Submission date	2024-03-08
Version	1.0

Related WP	WP4	Dissemination Level	PU
Lead Participant	GUF	Lead Author	Atiyeh Sadeghi, Kai Rannenberg (GUF)
Contributing Participants	UMA, ACEEU	Related Deliverables	D.4.1, D2.2, D.2.3, D3.1

Abstract: This deliverable presents the outcomes of Task T4.3 up to Month 15 (February 2024). Hence, it comprehensively records all CSP modules corresponding to the Cybersecurity Principle and Management Capability implemented by the end of February 2024. Moreover, it describes the context of the documentation task and the documentation methodology including the definition of a record comprising the relevant information per module.

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

This deliverable presents the outcomes of Task T4.3 “Operating the training modules on Cybersecurity Principles and Management” up to Month 15 (February 2024). It documents all CSP Modules corresponding to the Cybersecurity Principle and Management Capability implemented by the end of February 2024. Moreover, it describes the context of the documentation task and the documentation methodology including the definition of a record comprising the relevant information per module.
In order to develop D4.2 we followed the process specified below:

- We used the template for describing CSP modules from D4.1 and added the additional elements for the purposes of D4.2, i.e. the documentation of implemented CSP modules.
- We then documented the CSP modules covering the cybersecurity principles and management capability and implemented by M15 using a provisional tool developed by ACEEU, as the DCM is not yet available.

Document information

Contributors

Name	Beneficiary
Kai Rannenberg, Atiyeh Sadeghi	GUF
Cristina Alcaraz	UMA
Thorsten Kliewe, Jeldo Meppen	ACEEU

Reviewers

Name	Beneficiary
Javier Lopez	UMA
Sebastian Pape	SEA
Jeldo Meppen	ACEEU (as QM)

History

Version	Date	Contributor(s)	Comment(s)
0.01	2023-11-13	Kai Rannenberg, Atiyeh Sadeghi	1st Draft of ToC
0.02	2023-11-17	Kai Rannenberg, Atiyeh Sadeghi	Improved ToC reflecting comments and feedback from partners
0.03	2023-12-07	Kai Rannenberg, Atiyeh Sadeghi	Update on Section 2
0.04	2023-12-20	Vasco Delgado-Gomes, Kai Rannenberg, Atiyeh Sadeghi	WP3-WP4 Alignment template
0.05	2024-01-09	Nineta Polemi, Christos Douligeris	High-level review

0.06	2024-01-11	Kai Rannenberg, Atiyeh Sadeghi	Improvement based on high-level review comments
0.07	2024-02-08	Kai Rannenberg, Atiyeh Sadeghi	Improvement based on the 1st review comments
0.08	2024-02-22	Kai Rannenberg, Atiyeh Sadeghi	Improvement based on the 2nd review comments
0.09	2024-03-01	Kai Rannenberg, Atiyeh Sadeghi	Further improvement, especially based on a re-review of the KPIs in the GA
1.0	2024-03-07	Atiyeh Sadeghi	Final check, layout refinement and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**A**	Advanced
	ACEEU	ACEEU GmbH
	AIT	AIT Austrian Institute of Technology GmbH
	APIRO	ApiroPlus Solutions Ltd
B	**B**	Basic
C	**C**	Course
	C2B	C2B Consulting
	CNR	Consiglio Nazionale Delle Ricerche (National Research Council)
	CoA	Certificate of Attendance
	COFAC	COFAC Cooperativa de Formacao e Animacao Cultural CRl
	CS-E	Cybersecurity exercise
	CSP	CyberSecPro
D	**D**	Deliverable
	DCM	Dynamic Curriculum Management
E	**ECSF**	European Cybersecurity Skills Framework
F	**FCT**	Universidade NOVA de Lisboa (NOVA University of Lisbon)
	FTPS	File Transfer Protocol Secure
	FP	Focal Point
G	**GUF**	Johann Wolfgang Goethe-Universitaet Frankfurt am Main (Goethe University Frankfurt)
H	**H**	Hackathon
I	**ITML**	Information Technology for Market Leadership
	IMT	Institut Mines-Telecom
K	**KA**	Knowledge Area

L	**LAU**	Laurea-Ammattikorkeakoulu Oy (Laurea University of Applied Sciences)
M	**MAG**	Maggioli Spa
O	**O**	Other
P	**PDMFC**	Pdm e fc Projecto Desenvolvimento Manutencao Formacao e Consultadorialda
S	**S**	Seminar
	SEA	Social Engineering Academy
	SFTP	Secure File Transfer Protocol
	SGI	Serious Games Interactive ApS
	SINTEF	Sintef AS [SINTEF is not an acronym anymore, so the full name is SINTEF Aksjeselskap]
	SLC	Security Labs Consulting Limited
	SS	Summer School
	SVN	Subversion
T	**T**	Task
	TalTech	Tallinna Tehnikaülikool (Tallinn University of Technology)
	TRUSTILIO	trustilio B.V.
	TUBS	Technische Universitaet Braunschweig (Technical University of Braunschweig)
	TUC	Polytechneio Kritis (Technical University of Crete)
U	**UCY**	University of Cyprus
	UMA	Universidad de Malaga (University of Malaga)
	UNINOVA	Uninova-Instituto de Desenvolvimento de Novas Tecnologiasassociacao (UNINOVA - Institute for the Development of New Technologies)
	UNSPMF	University of Novi Sad Faculty of Sciences
	UPRC	University of Piraeus Research Center
V	**VPN**	Virtual Private Network

W	**W**	Workshop
	WP	Work Package
Z	**ZELUS**	Zelus IKE

1 Introduction

This section is structured as follows: Section 1.1 provides an overview of the background of the CSP project. In Section 1.2, the purpose and scope of WP4 and specially T4.3 are elaborated. Section 1.3 discusses the interrelation with other work packages and deliverables. Additionally, in Section 1.4, a brief outline of the subsequent sections' structure and organization is presented, offering readers a roadmap for navigating through this deliverable.

1.1 Background

Cybersecurity will persist be as a major issue in the foreseeable future for companies and industries across all sectors: Due to digitalized environment, increasing shortage of skilled professionals capable of fulfilling specific roles and duties within cybersecurity could be foreseen which is a significant concern for cybersecurity professionals. It is crucially important to provide comprehensive training for the next generation of professionals in order to effectively address the demanding and continually expanding cybersecurity landscape. By bridging the gap between academia and industry, CyberSecPro is poised to lead the charge in driving a culture of innovation and resilience in the digital realm, ensuring a safer and more secure future for all.

Hence, the CyberSecPro project aims to introduce a distinctive professional training program featuring cutting-edge hands-on training modules. These modules are to cater to diverse training requirements and proficiency levels, encompassing both general and sector-specific modules for sectors such as maritime, health, and energy industries.

1.2 Purpose and Scope

This deliverable was produced within the context of CyberSecPro Work Package 4, titled "*Operating CyberSecPro Professional Training Program*". Its high-level objective is to establish the documentation for each CSP module offer. This deliverable document the implemented CSP modules managed by Task 4.3 (T4.3), which are most of the modules on cybersecurity principles and management capabilities (some of those are managed by T4.4 due to the overlap with the capabilities on cybersecurity tools and technologies).

1.3 Relation to Other Work Packages and Deliverables

The primary objective of Work Package 4 "*Operating CyberSecPro Professional Training Program*" is to plan in detail the scalable offering and the operation of the CyberSecPro professional modules. This WP interacts with the other CyberSecPro work packages as follows: it receives content-oriented information (e.g., knowledge areas) from WP2 and syllabus-oriented information from WP3. In turn, WP4 delivers information to WP3 about the templates to describe implemented CyberSecPro modules.

This deliverable, D4.2, is related to D2.2 (CSP training supply), D2.3 (CSP knowledge areas), D3.1 (Logistics, syllabus aspects of templates and final CSP module design) and D4.1 (originally planned supply of modules in the CSP knowledge areas).

1.4 Structure of the Deliverable

The deliverable is organized as follows. Section 2 explains the overall methodological approach as well as the template used for documenting implemented CSP modules. In Section 3, we document the basic

and advanced general and sector-specific CSP modules on cybersecurity principles and management implemented by M15. Section 4 concludes the document.

2 Methodology

This section is structured as follows: Section 2.1, provides a brief overview of the CSP Modules that are relevant to cybersecurity principles and management, thereby aligning with T4.3. Section 2.2, elaborates on the template utilized for documenting implemented CSP Modules. In Section 2.3, reference is made to the template for offering CSP modules as provided in D3.1. Lastly, Section 2.4, introduces a provisional method for documenting implemented CSP Modules until the Dynamic Curriculum Management (DCM) becomes available.

2.1 CSP Modules on Cybersecurity Principles and Management

In this section, we will describe briefly which CSP Modules are related to cybersecurity principles and management and therefore to T4.3 titled "*Operating the training modules on Cybersecurity Principles and Management*". Based on Table 1, derived from D4.1, this task, T4.3, is responsible for the modules *CSP001 "Cybersecurity Essentials and Management", CSP002"Human Factors and Cybersecurity*", and *CSP005 "Data Protection and Privacy Technologies*". As shown in Table 1, the module *CSP003* "*Cybersecurity Risk Management and Governance*" is related to Knowledge Area 3 (KA3) and Knowledge Area 4 (KA4) covering the Capabilities categories cybersecurity tools and technologies and cybersecurity principles and management respectively. Therefore, the module *CSP003* "*Cybersecurity Risk Management and Governance*" will be covered partially by T4.3 and this deliverable, D4.2, partially by T4.4 and D4.3 (see more details below). T4.4 is responsible for operating the training modules on Cybersecurity tools. Documentation of the implemented CSP modules related to Knowledge Area 4 is covered in this deliverable, and documentation of the implemented CSP modules related to Knowledge Area 3 will be covered in D4.3.

Table 1: The interrelation between CSP Knowledge Areas, Capabilities categories and Module(s)*

CSP Knowledge Area	Capabilities category	Module(s)
CSP Knowledge Area 1 – Cybersecurity Management	Cybersecurity Principles and Management	CSP001 "Cybersecurity Essentials and Management"
CSP Knowledge Area 2 – Human Aspects of Cybersecurity	Cybersecurity Principles and Management	CSP002 "Human Factors and Cybersecurity"
CSP Knowledge Area 3 – Cybersecurity Risk Management	Cybersecurity Tools and Technologies	CSP003 "Cybersecurity Risk Management and Governance"
CSP Knowledge Area 4 – Cybersecurity Policy, Process, and Compliance	Cybersecurity Principles and Management	
CSP Knowledge Area 5 – Network and Communication Security	Cybersecurity Tools and Technologies	CSP004 "Network Security"
CSP Knowledge Area 6 – Privacy and Data Protection	Cybersecurity Principles and Management	CSP005 "Data Protection and Privacy Technologies"

CSP Knowledge Area 7 – Cybersecurity Threat Management	Cybersecurity Tools and Technologies	CSP006 "Cyber Threat Intelligence"
CSP Knowledge Area 8 – Cybersecurity Tools and Technologies	Cybersecurity in Emerging Digital Technologies	CSP007 "Cybersecurity in Emerging Technologies" CSP008 "Critical Infrastructure Security" CSP009 "Software Security"
CSP Knowledge Area 9 – Penetration Testing	Offensive Cybersecurity Practices	CSP010 "Penetration Testing" CSP011 "Cyber Ranges and Operations"
CSP Knowledge Area 10 – Cyber Incident Response	Offensive Cybersecurity Practices	CSP011 "Cyber Ranges and Operations" CSP012 "Digital Forensics"

* Cyan colour indicates the KAs covered by T4.3 and in this deliverable, D4.2.

CSP001 "Cybersecurity Essentials and Management"
This module can be related to the CSP KA1: Cybersecurity Management. This area delves into the principles and practices associated with the oversight of cybersecurity risks and programmes. Additionally, this module can be related to the knowledge areas Cybersecurity Management Systems, Cybersecurity Principles, and Cybersecurity Education and Training, among others.
CSP002 "Human Factors and Cybersecurity"
This module can be related to the CSP KA2: Human Aspects of Cybersecurity. This area explores the impact of human behaviour on cybersecurity and underscores the importance of security awareness training. Additionally, this general module can be related to knowledge areas Cybersecurity Education and Training, Soft and Transferable Skills, among others.
CSP003 "Cybersecurity Risk Management and Governance"
This module can be related to the CSP KA3: Cybersecurity Risk Management and CSP KA4: Cybersecurity Policy, Process and Compliance. These areas involve recognising, evaluating, and mitigating cybersecurity risks, as well as encompass the creation and implementation of cybersecurity policies and procedures and the management of cybersecurity compliance, respectively. Additionally, this module can be related to the knowledge areas Cybersecurity Risk Assessment and Management, Cybersecurity Regulations and Compliance, Legal and Auditing Training, among others. This deliverable, D4.2, only covers the part related to CSP KA 4 (see Table 1)
CSP005 "Data Protection and Privacy Technologies"
This module can be related to the CSP KA6: Privacy and Data Protection. This area addresses the principles and strategies aimed at preserving the privacy and confidentiality of data. Additionally, this module can be related to the knowledge area Data Protection and Security, among others.

2.2 Template for the Documentation of Implemented CSP Modules

In this section, we have used the template for describing CSP modules from D4.1. We have added additional elements needed for the documentation of implemented CSP modules as shown in Table 2. We have also synchronized this template with the descriptions for training modules D3.1.

Table 2: Template for the documentation of implemented CSP Modules

CSP Module Elements	CSP Module fields legend	CSP Module information
Code	**Code** (mandatory) *Code format:* *For general modules: CSP[n]_x* *[n] is the CSP module number (currently between 001 and 012)* *x is the module offering type (see below)* *For sector-specific modules: CSP[n]_x_y* *[n] is the CSP module number (currently between 001 and 012)* *x is the module offering type (see below) and y is the sector (E, H, M)*	
Content	**Module title as defined in the CSP catalogue** (mandatory) *The title of the module as defined in the CSP catalogue (currently in D4.1)*	
	Title of the implemented CSP module (mandatory) *The title of the implemented CSP module (instantiation of the designed module), probably one of the alternative titles mentioned in D3.3, D3.4 or D3.5, but in any case, one that can be proven after the implementation, e.g. from local documentation.*	
	Description of the implemented CSP module (mandatory) *Usually, the module description from the syllabus (D3.1), but if applicable enhanced with a description of the specialisations and modifications of this specific module*	
	Related knowledge area(s) (mandatory) *Mapping to the 10 selected CSP knowledge areas defined in D2.3*	

	Indicate whether in the implemented CSP module, learners learned how to implement EU cybersecurity standards, policy and regulatory principles as required to report on the respective KPI for impact/outcome (mandatory) *Yes (also if a part of the module covered this topic) or No (otherwise)*	
	Category/ies of capabilities (mandatory) *Mapping to the 4 category/ies of capabilities defined in the CSP Grant Agreement.*	
	Learning outcomes and targets (mandatory) *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module, with a reference to the syllabus as defined in D3.1*	
	Type of the implemented CSP module (mandatory) *Indicates the module type (delivery method) based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other (O) is chosen, the specific type is to be described in free text.*	
	Information on the sector (mandatory) *Indicates General, Maritime, Health, or Energy*	
	Pre-requisites (mandatory) *Information on knowledge, skills and competences required or useful for understanding the content of the implemented CSP module (usually taken from the syllabus (D3.1) but if applicable enhanced with specifics of this specific module)*	
	Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of the implemented CSP module within the ECSF (currently in this*	

	link). *It also indicates which of the (12) ECSF profiles are supported by this implemented CSP module (usually taken from the syllabi in D3.1, but if applicable enhanced with specifics of this specific implemented CSP module)*	
	Provision type and location (mandatory) *Indicates physical, virtual, or both. If physical, provide details about the location (country, city/village). If virtual, provide the URL link of the website*	
	Types of assignments *Programming task, essay, presentation, test-exam, mutual peer-review among students, other*	
	Level (mandatory) *B (Basic), A (Advanced)*	
	Language (mandatory) *Indicates the spoken and the language**s** for the material and the assessment/evaluation*	Spoken: Material: Assessment:
Management /Logistics	**Provider(s)** (mandatory) *Name(s) of the providing organisation(s), e.g. beneficiary/ies*	
	Contact (mandatory) *Full name(s) of the main contact person(s) including their email address*	
	Trainer(s) *All trainers with full name (potentially including title), name of organisation and position in organisation including key expertise and/or achievements in 1-2 sentences outlining why the person is capable/suitable for providing the training*	
	Tool(s) used (mandatory) *A list of tools that have been used for the implemented CSP module*	

	Required to report on CSP's KPI mentioned under SO 3.1 in the Grant Agreement that "at least 30 technological instruments will be used in the CyberSecPro training program"		
	Registration procedure *How (e.g. where and when registration of learner took place) did learner have to register*		
	Admission criteria *Limits of admission (if any), requirements and selection criteria, e.g. knowledge prerequisites, e.g. modules that learners need to have attended before or knowledge that is essential to understand the course (e.g. basics of cryptography or security management).*		
	ECTS *The number of ECTS*		
	Certificate of Attendance (CoA) (mandatory) *Indicates Yes or No (and the conditions for yes, e.g. partial or full attendance, passing of exam)*		
	Exact dates, when offered (mandatory) *Indicates the dates* (year, month, day) *for the schedule of the implemented CSP module, as well as periodicity (e.g., even after the end of the CSP project). If exam dates are significantly later than the teaching times, they should be mentioned as an additional piece of information*		
	Schedule and Duration (mandatory)	*Duration of the implemented CSP module (in hours)*	
		Duration of prefabricated teaching video(s) from the CSP module used in the implementation (in hours)	
		Estimated duration for students online-interaction	

		during the implemented CSP module (in hours)	
		Frequency, duration (in hours), and rhythm of assignments if applicable	
Materials	**Location of the learning and training materials, incorporating text and multimedia, e.g. manuals, video tutorials, and interactive guides** *Link to DCM once available, otherwise other link*		
	Location of activity modules, such as forums, quizzes, and assignments *Link to DCM once available, otherwise other link*		
	Location of community support *Link to DCM once available, otherwise other link*		
	Location of administrator documentation and configuration guides of tools used *Link to DCM once available, otherwise other link*		
Outcomes	**Learners enrolled** (mandatory) *Number of learners*		
	Number of learners per gender (mandatory) *Indicate per female, male, non-binary*		
	Number of learners per category (mandatory) *Covered categories: Students, academic personnel, employers, employees, practitioners, developers, officers (in absolute numbers). Each learner can belong to more than one category.*		
	Learners' background (mandatory) *Provides characteristics of learners, especially the following details, as they relate to CSP's*		

	KPIs: • *Number of learners more than 45 years old* • *Number of learners, who are non-ICT graduates* • *Number of learners, who are cybersecurity self-trained* *In the collection form this need to be 4 mandatory fields: One in free text to describe the scenario, 3 each asking for a figure to enable adding up the figures for the KPIs.*	
	Evaluation method(s) (mandatory) *Method for the evaluation of learner performance (indicates physical and/or virtual tests, participation, exercises, etc.)*	
	Number of evaluation forms filled by learners (mandatory)	
	Evaluation forms of learners (mandatory) *The form that learners used to evaluate the course offer (reference or link)*	
	Evaluation forms of trainers (mandatory) *The form that trainers used to evaluate the outcomes (reference or link)*	
	Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes (text or reference)*	
Financial information (possibly confidential depending on the decision of the provider)	**Income** (mandatory)	
	Scholarships/sponsorships (mandatory) *Number of waived (payable) registrations* *In the collection form this need to be 2 mandatory fields: One in free text to describe the scenario, one asking for a figure to enable adding up the figures for the KPIs.*	

	Cost-benefit analysis of the modules *The amount of money paid for the course and the amount of income earned from the course*	
Recommendations for Best Practices **Brief suggestions to enhance the effectiveness of CSP training (Lessons learnt)**	**Recommendations for improving the module** *Brief practical suggestions to elevate and improve the future CSP training module quality*	*For example:* • *Enhance the training module with more interactive exercises.* • *Continuously update the module with the latest cybersecurity trends.*
	Recommendations for expanding the reach of the module *Brief practical suggestions to expand the reach to a wider audience and diversifying delivery methods*	*For example:* • *Partner with industry.* • *Promote the module through targeted marketing.*
	Recommendations for future initiatives *Brief practical suggestions and future recommendation for proactive strategies to further strengthen cybersecurity training initiatives and address emerging challenges*	*For example:* • *Implement Standard Cybersecurity Framework in syllabi.* • *Foster collaboration with industry clusters for ongoing professional development opportunities for the participants of the training.* • *Foster EU member state collaboration on cybersecurity training offerings.*

2.3 Template for Planning the Offering of CSP Modules

A template for the offering of CSP Modules is provided in D3.1 “CyberSecPro programme main components and procedures” and later (once the DCM is available) in the DCM.

2.4 Reporting Method(s)

One of the challenges found during the operation phase has been to precisely establish the type of resource, method or tool necessary for the centralization of data documenting the implemented CSP modules and its sharing without depending on external management entities. Sensitive data, such as financial data, scholarships or particular restrictions of each entity, must be protected in several aspects, taking care of the confidentiality, integrity and availability of such data.

In addition, D4.2 which needs to document reports and training material on the cybersecurity principles and management training modules is due by M15. Beyond M15 the documentation will be continued as appropriate, possibly in the DCM, the periodic reports, or an update of D4.2, as applicable.

At least for the time, until the DCM becomes available, a provisional method is needed to document the implemented CSP modules. Exploring the various existing mechanisms without dependence on external entities and based on collaborative solutions (e.g., web forms, online excels or docs, online repositories, etc.), we found several strategies that can be adapted for our purpose, such as:

- Strategy 1: Sharing information using the most common means such as e-mail.
- Strategy 2: Setting up security mechanisms to establish secure point-to-point communications for information transference (e.g., a Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP), File Transfer Protocol Secure (FTPS), etc.).
- Strategy 3: Install or depend on on-premises repositories such as the SubVersioN (SVN) [1] provided by the coordinator for the CyberSecPro project or other similar ones such as OwnCloud [2] or NextCloud [3]. In this way, entities can centralise their information on a common server, and manage their own data at all times. Moreover, among the services offered by NextCloud, one can find remote collaboration applications that also benefit cooperation and interaction.
- Strategy 4: Implement centralised but customised ad hoc solutions according to the needs of the moment, and through a private server under limited access. This feature benefits the process of expanding capabilities or services that may be required to cover particular solutions that may arise at any given time.
- Strategy 5: Expanding Strategy 4 but focusing on a dynamic web platform, such as the DCM platform, which can be accessible under controlled policies and procedures.
- Strategy 6: Using a platform like GitLab [4] or any other web frontend for git, as it would combine the advantages of Strategies 4 and 5 with the possibility to use standard clients such as git.

Beyond these solutions and their corresponding advantages, there are also certain limitations that must be considered:

- Strategies 1 and 2: Both scenarios are not suitable for the CSP project, which is composed of several partners interacting with each other. They must cooperate to lead common purposes that must be transparent for all those involved, for example, in a common training module. Any constraints that may deviate from centralization and the provision of (semi-)interactive solutions may lead to unforeseen delays, conflicts, confusions or overlaps.
- Strategy 3: This scenario favours the centralisation of data, but does not allow the use of interactive solutions (with the exception of certain applications such as NextCloud) that facilitate the updating of such data from a collaborative and non-overlapping perspective. Moreover, Strategies 2 and 3 require entities/end users to install, maintain and apply client software components, which can be cumbersome or tedious to use.
- Strategies 4, 5, and 6: Fortunately, all three strategies are well suited for CSP since they facilitate to create customized solutions according to the needs. However, any customisation process

involves costs in terms of effort and time, especially in the case of Strategy 5, where the implementations must cover a wide range of technical requirements.

For this reason, and while the DCM platform is being finalised and tested, we consider Strategy 4 by extending the capacities of the CSP internal web (https://admin.cybersecpro-project.eu) and implementing the template described in Section 2.2 via a (semi-)interactive tool for module providers. Figure 1 shows the screenshot from the system provided by ACEEU. The system is available via:

https://admin.cybersecpro-project.eu/implementedmodules/listimplementedmodules

If providers of modules like to combine the content of several modules into one programme (or course or similar depending on local terminology), then for each module, whose content is used, one entry is to be made in the system.

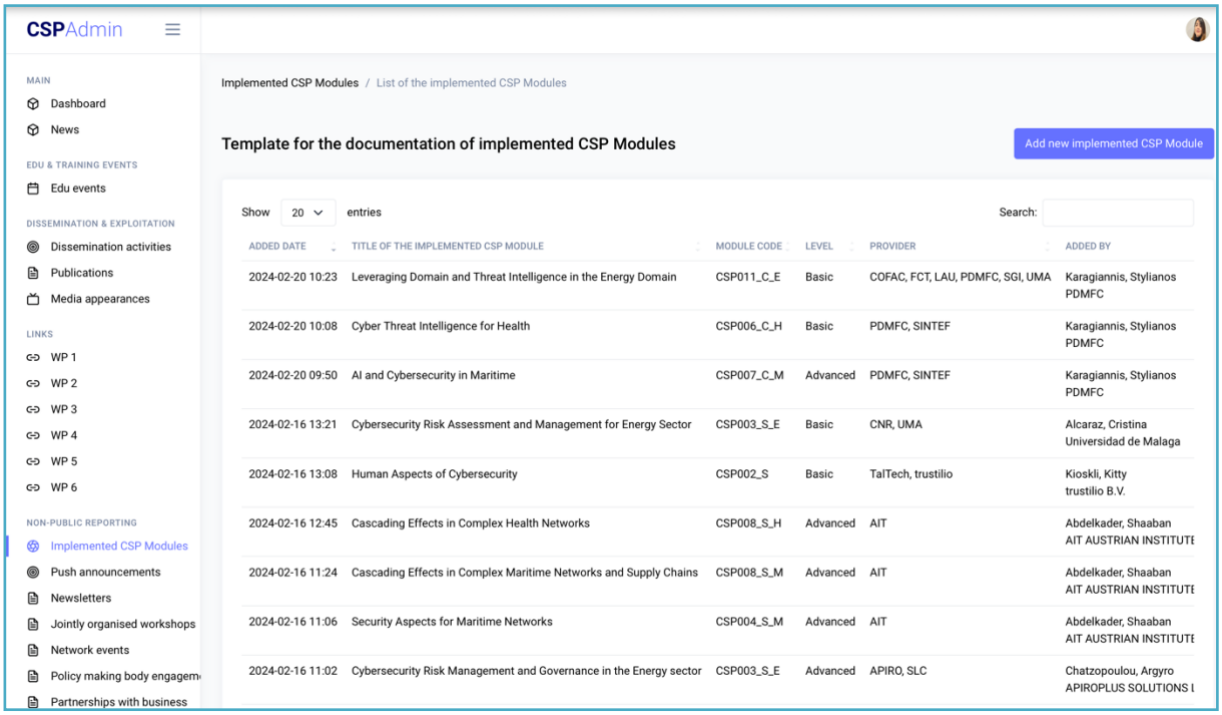

Figure 1: Screenshot from the system provided by ACEEU

3 Documentations of Implemented CSP Modules

This section records the CSP modules corresponding to the Cybersecurity Principle and Management Capability implemented by the end of M15 (February 2024).

3.1 General Cybersecurity Modules

3.1.1 General Cybersecurity Modules (Basic)

3.1.1.1 Tallinna Tehnikaülikool (TALTECH), Estonia

3.1.1.1.1 Human Aspects of Cybersecurity

CSP Module Elements	CSP Module fields legend	CSP Module information
Code	**Code** (mandatory) *Code format:* *For general modules: CSP[n]_x* *[n] is the CSP module number (currently between 001 and 012)* *x is the module offering type (see below)* *For sector-specific modules: CSP[n]_x_y* *[n] is the CSP module number (currently between 001 and 012)* *x is the module offering type (see below) and y is the sector (E, H, M)*	CSP002_S
Content	**Module title as defined in the CSP catalogue** (mandatory) *The title of the module as defined in the CSP catalogue (currently in D4.1)*	CSP002 - Human Factors and Cybersecurity
	Title of the implemented CSP module (mandatory) *The title of the implemented CSP module (instantiation of the designed module), probably one of the alternative titles mentioned in D3.3, D3.4 or D3.5, but in any case, one that can be proven after the implementation, e.g. from local documentation.*	Human Aspects of Cybersecurity

	Description of the implemented CSP module (mandatory) *Usually, the module description from the syllabus (D3.1), but if applicable enhanced with a description of the specialisations and modifications of this specific module*	This course dives deep into the human elements of cybersecurity, exploring the psychological, social, and organisational factors that influence security behaviours and decisions. Participants will gain insights into the human vulnerabilities that cyber attackers exploit and learn strategies to foster a culture of cybersecurity within organisations. It also emphasises the critical role of communication and collaboration at strategic, operational, and tactical levels. Participants will explore how effective communication across domains and decision-making processes can bolster cybersecurity efforts.
	Related knowledge area(s) (mandatory) *Mapping to the 10 selected CSP knowledge areas defined in D2.3*	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
	Indicate whether in the implemented CSP module, learners learned how to implement EU cybersecurity standards, policy and regulatory principles as required to report on the respective KPI for impact/outcome(mandatory) *Yes (also if a part of the module covered this topic) or No (otherwise)*	Yes

	Category/ies of capabilities (mandatory) *Mapping to the 4 category/ies of capabilities defined in the CSP Grant Agreement.*	Cybersecurity in Emerging Digital Technologies Cybersecurity Principles and Management Cybersecurity Tools and Technologies
	Learning outcomes and targets (mandatory) *A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module, with a reference to the syllabus as defined in D3.1*	In this program, aimed at cybersecurity professionals, participants will develop and implement effective communication strategies tailored specifically for cybersecurity contexts. They will learn to collaborate with cross-functional teams to address the human aspects of cybersecurity, analyzing real-world incidents to identify communication breakdowns and human factors. Participants will also gain the ability to categorize adversaries and analyze their profiles. The program will focus on building competencies such as leading and participating in strategic, operational, and tactical cybersecurity discussions, fostering a culture of open communication and collaboration, making informed cybersecurity decisions grounded in a comprehensive understanding of human aspects, and identifying and mitigating human threats and vulnerabilities effectively.
	Type of the implemented CSP module (mandatory) *Indicates the module type (delivery method) based on: Course (C), Workshop (W), Seminar (S), Cybersecurity exercise (CS-E), Summer School (SS), Hackathon (H), Other (O). If other (O) is chosen, the specific type is to be described in free text.*	Seminar (S)
	Information on the sector (mandatory)	General

	Indicates General, Maritime, Health, or Energy	
	Pre-requisites (mandatory) *Information on knowledge, skills and competences required or useful for understanding the content of the implemented CSP module (usually taken from the syllabus (D3.1) but if applicable enhanced with specifics of this specific module)*	• Interest in human-centric cybersecurity • Basic understanding of computers and networking • Familiarity with common internet security threats and vulnerabilities • Awareness of cybersecurity
	Relevance to European Cybersecurity Skills Framework (ECSF) *An indicative relevance of the implemented CSP module within the ECSF (currently in this link). It also indicates which of the (12) ECSF profiles are supported by this implemented CSP module (usually taken from the syllabi in D3.1, but if applicable enhanced with specifics of this specific implemented CSP module)*	• Cybersecurity Educator • Cybersecurity Implementer • Cybersecurity Researcher • Cybersecurity Risk manager • Digital Forensics Investigator
	Provision type and location (mandatory) *Indicates physical, virtual, or both. If physical, provide details about the location (country, city/village). If virtual, provide the URL link of the website*	Virtual location: Link
	Types of assignments *Programming task, essay, presentation, test-exam, mutual peer-review among students, other*	Essay
	Level (mandatory) *B (Basic), A (Advanced)*	Basic
	Language (mandatory) *Indicates the spoken and the languages for the material and the assessment/evaluation*	Spoken: English Material: English Assessment: English

Management /Logistics	**Provider(s)** (mandatory) *Name(s) of the providing organisation(s), e.g. beneficiary/ies*	Tallin University of Technology (TalTech) trustilio B.V. (trustilio)
	Contact (mandatory) *Full name(s) of the main contact person(s) including their email address*	Kitty Kioskli (kitty.kioskli@trustilio.com) Ricardo Gregorio Lugo (ricardo.lugo@taltech.ee)
	Trainer(s) *All trainers with full name (potentially including title), name of organisation and position in organisation including key expertise and/or achievements in 1-2 sentences outlining why the person is capable/suitable for providing the training*	Kitty Kioskli (kitty.kioskli@trustilio.com) Ricardo Gregorio Lugo (ricardo.lugo@taltech.ee)
	Tool(s) used (mandatory) *A list of tools that have been used for the implemented CSP module* *Required to report on CSP's KPI mentioned under SO 3.1 in the Grant Agreement that "at least 30 technological instruments will be used in the CyberSecPro training program"*	Teams
	Registration procedure *How (e.g. where and when registration of learner took place) did learner have to register*	-
	Admission criteria *Limits of admission (if any), requirements and selection criteria, e.g. knowledge prerequisites, e.g. modules that learners need to have attended before or knowledge that is essential to understand the course (e.g. basics of cryptography or security management).*	-

	ECTS *The number of ECTS*		-
	Certificate of Attendance (CoA) (mandatory) *Indicates Yes or No (and the conditions for yes, e.g. partial or full attendance, passing of exam)*		No
	Exact dates, when offered (mandatory) *Indicates the dates* (year, month, day*) for the schedule of the implemented CSP module, as well as periodicity (e.g., even after the end of the CSP project). If exam dates are significantly later than the teaching times, they should be mentioned as an additional piece of information*		2024.01.15 2024.02.05
	Schedule and Duration (mandatory)	*Duration of the implemented CSP module (in hours)*	06.00 hours
		Duration of prefabricated teaching video(s) from the CSP module used in the implementation (in hours)	06.00 hours
		Estimated duration for students online-interaction during the implemented CSP module (in hours)	06.00 hours
		Frequency, duration (in hours), and rhythm of assignments if applicable	-
Materials	**Location of the learning and training**		-

	materials, incorporating text and multimedia, e.g. manuals, video tutorials, and interactive guides *Link to DCM once available, otherwise other link*	
	Location of activity modules, such as forums, quizzes, and assignments *Link to DCM once available, otherwise other link*	-
	Location of community support *Link to DCM once available, otherwise other link*	-
	Location of administrator documentation and configuration guides of tools used *Link to DCM once available, otherwise other link*	-
Outcomes	**Learners enrolled** (mandatory) *Number of learners*	40
	Number of learners per gender (mandatory) *Indicate per female, male, non-binary*	Male:35 Female:5 Non-binary:0
	Number of learners per category (mandatory) *Covered categories: Students, academic personnel, employers, employees, practitioners, developers, officers (in absolute numbers). Each learner can belong to more than one category.*	Students: 35 Academic Personnel: 5 Employers: 0 Employees: 0 Practitioners: 0 Developers: 0 Officers: 0
	Learners' background (mandatory) *Provides characteristics of learners, especially the following details, as they relate to CSP's KPIs:* • *Number of learners more than 45 years old* • *Number of learners, who are*	Number of learners more than 45 years: 5 Number of learners, who are non-ICT graduates: 0 Number of learners, who are cybersecurity self-trained: 15

	non-ICT graduates • *Number of learners, who are cybersecurity self-trained* *In the collection form this need to be 4 mandatory fields: One in free text to describe the scenario, 3 each asking for a figure to enable adding up the figures for the KPIs.*	
	Evaluation method(s) (mandatory) *Method for the evaluation of learner performance (indicates physical and/or virtual tests, participation, exercises, etc.)*	Essay
	Number of evaluation forms filled by learners (mandatory)	5
	Evaluation forms of learners (mandatory) *The form that learners used to evaluate the course offer (reference or link)*	TBA
	Evaluation forms of trainers (mandatory) *The form that trainers used to evaluate the outcomes (reference or link)*	TBA
	Evaluation and verification of learning outcomes *Assessment elements and high-level process to determine participants have achieved the learning outcomes (text or reference)*	-
Financial information (possibly confidential depending on the decision of the provider)	**Income** (mandatory)	Confidential
	Scholarships/sponsorships (mandatory) *Number of waived (payable) registrations* *In the collection form this need to be 2 mandatory fields: One in free text to describe the scenario, one asking for a figure to enable adding up the figures*	Confidential

	for the KPIs.	
	Cost-benefit analysis of the modules *The amount of money paid for the course and the amount of income earned from the course*	Confidential
Recommendations for Best Practices **Brief suggestions to enhance the effectiveness of CSP training (Lessons learnt)**	**Recommendations for improving the module** *Brief practical suggestions to elevate and improve the future CSP training module quality*	-
	Recommendations for expanding the reach of the module *Brief practical suggestions to expand the reach to a wider audience and diversifying delivery methods*	-
	Recommendations for future initiatives *Brief practical suggestions and future recommendation for proactive strategies to further strengthen cybersecurity training initiatives and address emerging challenges*	-

3.1.1.2 trustilio B.V. (trustilio), Netherlands

3.1.1.2.1 Human Aspects of Cybersecurity

See 3.1.1.1.1 Human Aspects of Cybersecurity

3.1.2 General Cybersecurity Modules (Advanced)

3.2 Sector-specific Cybersecurity Modules

3.2.1 Health Cybersecurity Modules (Basic)

3.2.2 Health Cybersecurity Modules (Advanced)

3.2.3 Energy Cybersecurity Modules (Basic)

3.2.4 Energy Cybersecurity Modules (Advanced)

3.2.5 Maritime Cybersecurity Modules (Basic)

3.2.6 Maritime Cybersecurity Modules (Advanced)

4 Summary and Conclusion

This deliverable presents the outcomes of Task T4.3 up to Month 15 (February 2024). Hence, it comprehensively records all CSP modules corresponding to the Cybersecurity Principle and Management Capability implemented by the end of February 2024. Moreover, it describes the context of the documentation task and the documentation methodology including the definition of a record comprising the relevant information per module. For the time until the DCM is available to collect and retrieve this information, ACEEU has established a system to document all implemented CSP modules. By the end of February 2024, one CSP module had been successfully implemented, as detailed in Section 3.1. The documentation will be continued beyond M15 as appropriate, possibly in the DCM, the periodic reports, or an update of D4.2, as applicable.

References

[1] “Apache Subversion,” [Online]. Available: https://subversion.apache.org/. [Accessed 20 February 2024].

[2] OwnCloud GmbH," OwnCloud," [Online]. Available: https://owncloud.com. [Accessed 26 January 2024].

[3] NextCloud GmbH," NextCloud," [Online]. Available: https://nextcloud.com. [Accessed 26 January 2024].

[4] GitLab Inc., “GitLab,” [Online]. Available: https://about.gitlab.com . [Accessed 04 March 2024].