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

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

# D3.1
# CyberSecPro Programme Main Components and Procedures

| Document Identification | |
|---|---|
| Due date | 2024-02-29 |
| Submission date | 2024-03-15 |
| Re-submission date | 2024-12-06 |
| Version | 1.6 |

| | | | |
|---|---|---|---|
| Related WP | WP3 | Dissemination Level | PU |
| Lead Participant | UNINOVA | Lead Author | Paresh Rathod (LAU), Paulinus Ofem (LAU), Vasco Delgado-Gomes (UNINOVA) |
| Contributing Participants | GUF, IMT, LAU, TalTech, TUBS, TUC, UCY, UMA, AIT, CNR, UPRC, APIRO, FP, ITML, MAG, PDMFC, SLC, TRUSTILIO, ZELUS, FCT | Related Deliverables | D2.3, D4.1, D4.2 |

**Abstract:** This deliverable outlines the main components and procedures of the CyberSecPro (CSP) programme. This document presents the CSP programme's general-purpose or model syllabi with its training modules and the Dynamic Curriculum Management (DCM) system. This deliverable reflects the outcomes of tasks T3.1 and T3.2. It focuses on the CSP training modules, model syllabi, templates, and key elements of the individual training modules specifically tailored to the health, energy, and maritime sectors. The online DCM portfolio encompasses various training modules, including general academic courses, online courses, training, workshops, cyber exercise sessions, sector-specific seminars, hackathons, and interactive cybersecurity labs. The outcomes are a model syllabus for CSP's main 12 generic training modules.

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.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

# Executive Summary

This deliverable outlines the CyberSecPro (CSP) programme's main components and procedures. The focus is on CSP training modules and model syllabi, templates, and key elements of the individual training modules. More details specifically tailored to the health, energy, and maritime sectors will be described in deliverables D3.3, D3.4 and D3.5. Building upon the WP2's general CSP programme design, the interrelationships among these components are analysed to ensure that the teaching objectives are realistic, achievable, and aligned with the CSP Knowledge Areas (KAs) while equipping participants with market-oriented capabilities. Additionally, detailed enrolment procedures were established, and various templates and e-forms were developed. The CSP modules can be delivered in various formats, including instructor-led courses, online courses, blended learning approaches, general academic courses, professional training, workshops, cyber exercise sessions, sector-specific seminars, hackathons, and interactive cybersecurity labs.

Under T2.3 requirements, the online Dynamic Curriculum Management (DCM) was integrated and envisioned by parameterising the Moodle platform, continuously monitoring cybersecurity market needs, and effectively managing the CSP syllabus and curriculum. The curriculum portfolio encompasses various training modules, including general academic courses, online courses, training, workshops, cyber exercise sessions, sector-specific seminars, hackathons, and interactive cybersecurity labs. The agile DCM efficiently manages the CyberSecPro programme portfolio, ensuring responsiveness to evolving needs. DCM also stores the general curricula and detailed syllabus tailored to the CSP KAs and learning targets developed in T3.1.

The outcome can benefit any higher education institution and training providers to base their offerings on this model syllabi developed with comprehensive research, innovation, and practitioners' contribution. The outcomes can be also model guideline for building the cybersecurity training and education programmes.

# Document information

## Contributors

| Name | Beneficiary |
|---|---|
| Vasco Delgado-Gomes, Paulo Figueiras, and Ruben Costa | UNINOVA |
| Paresh Rathod, Paulinus Ofem & others | LAU |
| N. Polemi, T. Karvounidis, C. Douligeris, D. Koutras, P. Kotzanikolaou, S. Papageorgiou, A. Andreatos | UPRC |
| K. Kioskli, L. Despotopoulou, M. Lambrou | Trustilio |
| A. Chatzopoulou, A. Karras | APIRO |
| Antonios Ntib | TUBS |
| Danijela Boberic Krsticev | UNSPMF |
| Spiros Borotis, Alexandros Rizopoulos | MAG |
| Pinelopi Kyranoudi | TUC |
| Shareeful Islam | SLC |
| S. Schauer, G. Langner, A. Shabaan | AIT |
| Ricardo G. Lug | TalTech |
| Elias Athanasopoulos | UCY |
| Cristina Alcaraz, Javier Lopez, Rodrigo Roman, Ruben Rios and Jose Antonio Onieva | UMA |

## Reviewers

| Name | Beneficiary |
|---|---|
| Per Håkon Meland and Nektaria Kaloudi | SINTEF |
| Ricardo Gregorio Lugo | TalTech |
| Theodoros Karvounidis | UPRC |
| Paulinus Ofem | LAU |

## History

| Version | Date | Contributor(s) | Comment(s) |
|---|---|---|---|
| 0.1 | 2023-08-18 | Vasco Delgado-Gomes | 1st Draft: ToC and initial sections with responsible partners. |
| 0.2 | 2023-08-29 | Paresh Rathod/Paulinus Ofem | Restructured Chapter 2 to reflect T3.1 objectives. |
| 0.3 | 2023-09-05 | Paresh Rathod | Restructured the ToC to aligned with CSP training modules. |
| 0.4 | 2023-09-07 | Nineta Polemi | Technical Inputs and consolidated ToC and Topics. |
| 0.5 | 2023-09-07 | Paresh Rathod | Consolidated technical manager’s recommendations. This is a final draft of ToC for the WP3 partners’ comments. |
| 0.6 | 2023-09-26 | Paresh Rathod, Theodoros Karvounidis, Paulo Figueiras | Agreed on CSP Modules & task allocations at Chania Meeting (September 25th & 26th, 2023) |
| 07 | 2023-10-18 | Paulinus Ofem, Vasco Delgado-Gomes, Paresh Rathod | Agreed on ToC, Work Allocations & Notify to PC and Technical Manager for final remark. |
| 08 | 2023-11-27 | Paresh Rathod, Vasco Delgado-Gomes, Cristina Alcaraz | PPT template and rationale and reviewing partners' inputs and consolidating some parts. |
| 0.9 | 2023-11-28 | Kai Rannenberg, Danijela Boberic Krsticev | Technical inputs on the syllabi of Modules 4, 5 and 7. |
| 0.10 | 2023-12-02 | Argyro Chatzopoulou, Apostolos Karras | Editorial inputs and review of sections 1 & 3.1. Technical input for Module 3. |
| 0.11 | 2023-12-03 | Bruno Bender | Partner Input – Penetration testing module. |
| 0.12 | 2023-12-06 | Antonios Ntib | Input- Module 3.4 & Module 3.5 |
| 0.13 | 2023-12-07 | Spiros Borotis | Partner input - sections 2.1.1, 2.1.3, 2.1.4. |
| 0.14 | 2023-12-07 | Pinelopi Kyranoudi | Technical input - Module 3.9. |
| 0.15 | 2023-12-08 | Shareeful Islam | Detailed description for the training module 6. |
| 0.16 | 2023-12-18 | Cristina Alcaraz | Comments to Module 1 and suggestions. |

| | | | |
|---|---|---|---|
| 0.17 | 2023-12-20 | Cristina Alcaraz, Javier Lopez, Rodrigo Roman, Ruben Rios | Detailed description for the training Module 4. |
| 0.18 | 2023-12-26 | Cristina Alcaraz, Javier Lopez | Detailed description of the presentations. |
| 0.19 | 2023-12-21 | N. Polemi, D. Koutras, P. Kotzanikolaou, S. Papageorgiou, T. Karvounidis, A. Andreatos | Review of all modules, contributions of Module 3, 11, 6, 8. |
| 0.20 | 2023-12-27 | K. Kioskli | Review and final contribution of Module 2. |
| 0.21 | 2023-12-27 | Paresh Rathod | Overall observation and assessing the need for consolidation work. |
| 0.22 | 2024-01-03 | Paresh Rathod, Paulinus Ofem | Consolidation work started: Template updates (comments from PC and partners considered). |
| 0.23 | 2024-01-25 | Vasco Delgado-Gomes | Version ready for high-level review. |
| 0.24 | 2024-01-30 | Paulinus Ofem | Updates: (1) Kai's suggested changes have been affected in GUF-related modules (2) Penetration testing has been revised and may still require some consolidation. (3) Section 3.13 has been drafted and may require further consolidation. |
| 0.25 | 2024-01-30 | Paresh Rathod, Paulinus Ofem | Consolidation. Review and integration of preparedness checklist and recommendations for video editors proposed by UMA. Integrated cyber range and operations workshop proposed by FCT. |
| 0.26 | 2024-02-10 | Paresh Rathod | Consolidation for Chapter 1, 2 and syllabus of the module-1 to module 2 in sections 3.1, 3.2 and 3.3. |
| 0.27 | 2024-02-11 | Paresh Rathod | Finalised the consolidation of all 12 modules syllabus in section 3.1 to 3.12. |
| 0.28 | 2024-02-12 | Paulinus Ofem | Reviewed and integrated input from UMA regarding Module 8. |
| 0.29 | 2024-02-13 | Paresh Rathod | Consolidated and ready for Review Round-2 |
| 0.30 | 2024-02-23 | Paulinus Ofem | - Reviewed and integrated input from Stefan of AIT.<br>- Addressed D3.1 Reviewers' (TalTech) comments regarding (Chapters 1 – 3, 5). |

| | | | |
|---|---|---|---|
| | | | - Addressed D3.1 Reviewers' (SINTEF) comments regarding Chapters 1 – 3, 5. |
| 0.31 | 2024-02-26 | Paresh Rathod | Final consolidation of the content of Chapters 1 to 3. The new sections on pedagogical aspects and soft skills been added in reference to D2.3. |
| 0.32 | 2024-02-27 | Vasco Delgado-Gomes | Final consolidation of Chapter 4 and 5.<br>Consolidation of Appendix tables with current information from CSP module declaration and D4.1 (CSP modules declaration - Google Sheets) |
| 0.33 | 2024-02-29 | Vasco Delgado-Gomes | Final formatting of the report for the consistency and professional report for EU project. Version ready for round 2 internal review. |
| 0.34 | 2024-03-01 | Vasco Delgado-Gomes | Version addressing round 2 internal reviewers comments. |
| 1.0 | 2024-03-01 | Vasco Delgado-Gomes | Final version submitted to PC, ready for EC submission. |
| 1.1 | 2024-03-2 – 2024-03-14 | Vasco Delgado-Gomes, Atiyeh Sadeghi | Layout corrections and improvements |
| 1.2 | 2024-03-15 | Ahad Niknia | Layout correction, improvement, preparation and submission process |
| 1.3 | 2024-06-03 | Vasco Delgado-Gomes, Ruben Costa, Paulo Figueiras, Paresh Rathod, Atiyeh Sadeghi | Added section 3.1.7 (Transperency Guidelines) and updated of the 4.10.1 (Template for planning the offering of CSP Modules). |
| 1.4 | 2024-11-15 | Vasco Delgado-Gomes, Ruben Costa, Paulo Figueiras | Updated section 3 introduction and the tables describing each training module. Also subsection 4.8 *Copying with Accessibility Issues* was added, based on the reviewers' comments received in the review report. |
| 1.5 | 2024-11-20 | Vasco Delgado-Gomes, Ruben Costa, Paulo Figueiras | Addressed internal reviewers' comments from Theodoros (UPRC) and Paulinus (LAU). |
| 1.6 | 2024-12-06 | Vasco Delgado-Gomes, Dimitris N. Kallergis | Additional inputs to address reviewers' comments. Final version submited to the PC. |
| 1.6 | 2024-12-06 | Ahad Niknia | Final check, preparation and submission process |

# Table of Contents

**Document information** ........ **v**
**1 Introduction** ........ **1**
**1.1 Goals** ........ **1**
**1.2 Methodology** ........ **2**
1.2.1 Criteria setting ........ 2
1.2.2 Process followed ........ 2
1.2.2.1 Phase 1: Modules Declaration Phase. ........ 2
1.2.2.2 Phase 2: Finalising CSP Programme ........ 3
1.2.3 Dynamic Nature of the CSP programme ........ 4
**2 CyberSecPro Programme and Value Proposition** ........ **5**
**2.1 Who Should Take CyberSecPro Training?** ........ **5**
**2.2 When Should You Take CyberSecPro Training?** ........ **6**
**2.3 Why You Need CyberSecPro Training?** ........ **6**
**2.4 Prerequisites and Requirements for Taking CyberSecPro Training** ........ **7**
**2.5 Pedagogical Aspects** ........ **8**
**2.6 Soft and Transversal Skills** ........ **10**
**3 CyberSecPro Generic Training Modules Syllabus** ........ **13**
**3.1 Module 1 - Cybersecurity Essentials and Management** ........ **13**
3.1.1 Target Audience and Goals ........ 13
3.1.2 Description of Training Module 1: Cybersecurity Essentials and Management ........ 14
3.1.3 Syllabus of the Training Module 1: Cybersecurity Essentials and Management ........ 20
3.1.4 CyberSecPro General Presentation Template for the Training Module ........ 22
3.1.5 CyberSecPro General Video Teaser template for the Training Module ........ 24
3.1.5.1 Analysis and recommendation of free and open-source video editors ........ 27
3.1.6 CyberSecPro Training Module Evaluation Template-Trainees and Trainers ........ 29
3.1.7 Transparency Guidelines- CyberSecPro Education and Training Material ........ 29
**3.2 Module 2 - Human Factors and Cybersecurity** ........ **31**
3.2.1 Target Audience and Goals ........ 31
3.2.2 Description of Training Module 2: Human Factors and Cybersecurity ........ 31
3.2.3 Syllabus of the Training Module 2: Human Factors and Cybersecurity ........ 37
**3.3 Module 3 - Cybersecurity Risk Management and Governance** ........ **39**
3.3.1 Target Audience and Goals ........ 39
3.3.2 Description of Training Module 3: Cybersecurity Risk Management and Governance ........ 40
3.3.3 Syllabus of Training Module 3: Cybersecurity Risk Management and Governance ........ 46
**3.4 Module 4 - Network Security** ........ **48**
3.4.1 Target Audience and Goals ........ 48
3.4.2 Description of Training Module 4: Network Security ........ 48

3.4.3 Syllabus of Training Module 4: Network Security ..... 55
**3.5 Module 5 - Data Protection and Privacy Technologies ..... 58**
3.5.1 Target Audience and Goals ..... 58
3.5.2 Description of Training Module 5: Data Protection and Privacy Technologies ..... 58
3.5.3 Syllabus of Training Module 5: Data Protection and Privacy Technologies ..... 63
**3.6 Module 6 - Cyber Threat Intelligence ..... 64**
3.6.1 Target Audience and Goals ..... 64
3.6.2 Description of Training Module 6: Cyber Threat Intelligence ..... 65
3.6.3 Syllabus of Training Module 6: Cyber Threat Intelligence ..... 71
**3.7 Module 7 - Cybersecurity in Emerging Technologies ..... 73**
3.7.1 Target Audience and Goals ..... 73
3.7.2 Description of Training Module 7: Cybersecurity in Emerging Technologies ..... 73
3.7.3 Syllabus of Training Module 7: Cybersecurity in Emerging Technologies ..... 79
**3.8 Module 8 - Critical Infrastructure Security ..... 81**
3.8.1 Target Audience and Goals ..... 81
3.8.2 Description of Training Module 8: Critical Infrastructure Security ..... 82
3.8.3 Syllabus of Training Module 8: Critical Infrastructure Security ..... 88
**3.9 Module 9 - Software Security ..... 90**
3.9.1 Target Audience and Goals ..... 90
3.9.2 Description of Training Module 9: Software Security ..... 90
3.9.3 Syllabus of Training Module 9: Software Security ..... 95
**3.10 Module 10 - Penetration Testing ..... 96**
3.10.1 Target Audience and Goals ..... 96
3.10.2 Description of Training Module 10: Penetration Testing ..... 97
3.10.3 Syllabus of Training Module 10: Penetration Testing ..... 102
**3.11 Module 11 - Cyber Ranges and Operations ..... 103**
3.11.1 Target Audience and Goals ..... 103
3.11.2 Description of Training Module 11: Cyber Ranges and Operations ..... 104
3.11.3 Syllabus of Training Module 11: Cyber Ranges and Operations ..... 109
**3.12 Module 12 - Digital Forensics ..... 111**
3.12.1 Target Audience and Goals ..... 111
3.12.2 Description of Training Module 12: Digital Forensics ..... 111
3.12.3 Syllabus of Training Module 12: Digital Forensics ..... 117
**3.13 Analysis of Interrelationships between Module Components ..... 118**
**4 CyberSecPro DCM Setup ..... 121**
**4.1 Moodle Parameterisation ..... 122**
4.1.1 Background ..... 122
4.1.2 Objectives ..... 122

4.1.2.1 Enhance user experience ... 122
4.1.2.2 Streamline administrative processes ... 122
4.1.2.3 Facilitate personalised learning paths ... 122
4.1.2.4 Ensure data security and compliance ... 122
4.1.2.5 Foster collaboration and engagement ... 122
**4.2 Moodle Overview ... 123**
4.2.1 Features and Capabilities ... 123
4.2.1.1 Course Management ... 123
4.2.1.2 Collaboration Tools ... 123
4.2.1.3 Assessment and Grading ... 123
4.2.1.4 Flexibility and Adaptability ... 123
4.2.1.5 Multimedia Integration ... 123
4.2.1.6 Accessibility ... 123
4.2.2 Importance in Education ... 123
4.2.2.1 Scalability ... 123
4.2.2.2 Cost-Effectiveness ... 123
4.2.2.3 Community Support ... 123
4.2.2.4 Pedagogical Flexibility ... 124
4.2.2.5 Data Security and Privacy ... 124
**4.3 Scope ... 124**
4.3.1 Defined Parameters ... 124
4.3.1.1 User Roles and Permissions ... 124
4.3.1.2 Course Structures and Taxonomies ... 124
4.3.1.3 Assessment and Grading Criteria ... 124
4.3.1.4 Integration with External Systems ... 124
4.3.2 Constraints and Limitations ... 125
4.3.2.1 Technical Constraints ... 125
4.3.2.2 Budgetary Limitations ... 125
4.3.2.3 Time Constraints ... 125
4.3.2.4 Stakeholder Acceptance ... 125
**4.4 DCM System Architecture ... 125**
4.4.1 Moodle Components ... 125
4.4.1.1 Core Components ... 125
4.4.1.1.1 Moodle Core ... 125
4.4.1.1.2 Database ... 125
4.4.1.1.3 User Interface ... 126
4.4.1.2 Modular Components ... 126
4.4.1.2.1 Plugins and Modules ... 126

4.4.1.2.2 Themes ..... 126
4.4.1.3 Integration Components ..... 126
4.4.1.3.1 External Integrations ..... 126
4.4.1.3.2 Application Programming Interfaces ..... 126
**4.5 Parametrisation Strategy ..... 126**
4.5.1 Customisation Requirements ..... 126
4.5.1.1 Course Customisation ..... 126
4.5.1.2 Institutional Branding ..... 127
4.5.2 User Roles and Permissions ..... 127
4.5.2.1 Role Definition ..... 127
4.5.2.2 Permission Assignment ..... 127
4.5.3 Data Migration Considerations ..... 128
4.5.3.1 Pre-Migration Preparation ..... 128
4.5.3.2 Migration Execution ..... 128
**4.6 Technical Details ..... 128**
4.6.1 Moodle Configuration Settings ..... 128
4.6.1.1 Site Administration ..... 128
4.6.1.2 Course and Activity Settings ..... 128
4.6.2 Plugin Integration ..... 129
4.6.2.1 Plugin Selection ..... 129
4.6.3 Database Configuration ..... 129
4.6.3.1 Database Selection ..... 129
**4.7 User Interface Design ..... 129**
4.7.1 Theme Customisation ..... 129
4.7.1.1 Theme Selection ..... 129
4.7.1.2 Theme Configuration ..... 129
4.7.2 Branding Elements ..... 130
4.7.2.1 Logo and Icons ..... 130
4.7.2.2 Messaging and Language ..... 130
**4.8 Training and Documentation ..... 130**
4.8.1 End-User Training ..... 132
4.8.1.1 Training Programmes ..... 132
4.8.1.2 End-User Support ..... 132
4.8.2 Administrator Documentation ..... 132
4.8.2.1 Configuration Guides ..... 132
**4.9 Logistics and Processes ..... 133**
4.9.1 Introduction ..... 133
4.9.2 User Authentication Process ..... 133

4.9.3 User Login Process ........ 133
4.9.4 User Logout Process ........ 133
4.9.5 Session Management and Security Measures ........ 134
4.9.6 Continuous Improvement and Adaptation ........ 134
4.9.7 Conclusion........ 134
**4.10 E-Forms ........ 134**
4.10.1 Template for planning the offering of CSP Modules........ 135
**5 Conclusions........ 139**
**References ........ 141**
**Annex A: CSP general modules declaration ........ 143**
**Annex B: Training offers in the 12 CSP modules........ 151**
**Annex C: CyberSecPro Training Module Evaluation Template: Training Participant ........ 157**
**Annex D: CyberSecPro Training Module Evaluation Template: Trainer ........ 161**
**Annex E: CyberSecPro Training Module Verification Template - Preparedness Checklist (a completion guideline for D3.3-D3.5)........ 165**

## List of Figures

Figure 1: Schematic overview on the value proposition for the CyberSecPro programme. 8

Figure 2: CyberSecPro PPT template. 24

Figure 3. Example to display the CC license logo (video teaser of the the CyberSecPro training module 1 for energy sector). 31

Figure 4: CyberSecPro DCM screenshot. 121

## List of Tables

Table 1: CyberSecPro recommended training delivery method. 8

Table 2: CyberSecPro recommended soft skills development practices. 11

Table 3: Cybersecurity essentials and management: Training Module 1 description. 14

Table 4: Cybersecurity essentials and management: Training Module 1 syllabus. 20

Table 5: Generic presentation template summary 23

Table 6: Generic video teaser development template. 25

Table 7: Essential features of video editors for creating video teasers. 28

Table 8: Human factors and cybersecurity: Training Module 2 description. 31

Table 9: Human factors and cybersecurity: Training Module 2 syllabus. 37

Table 10: Cybersecurity risk management and governance: Training Module 3 description. 40

Table 11: Cybersecurity risk management and governance: Training Module 3 syllabus. 46

Table 12: Network security: Training Module 4 description. 49

Table 13: Network security: Training Module 4 syllabus. 55

Table 14: Data protection and privacy technologies: Training Module 5 description. 58

Table 15: Data protection and privacy technologies: Training Module 5 syllabus. 63

Table 16: Cyber threat intelligence: Training Module 6 description. 65

Table 17: Cyber threat intelligence: Training Module 6 syllabus 71

Table 18: Cybersecurity in emerging technologies: Training Module 7 description 73

Table 19: Cybersecurity in emerging technologies: Training Module 7 syllabus. 79

Table 20: Critical infrastructure security: Training Module 8 description. 82

Table 21: Critical infrastructure security: Training Module 8 syllabus. 88

Table 22: Software security: Training Module 9 description. 90

Table 23: Software security: Training Module 9 syllabus. 95

Table 24: Penetration testing: Training Module 10 description. 97

Table 25: Penetration testing: Training Module 10 syllabus. 102

Table 26: Cyber ranges and operations: Training Module 11 description. 104

Table 27: Cyber ranges and operations: Training Module 11 syllabus. .......... 109
Table 28: Digital forensics: Training Module 12 description. .......... 111
Table 29: Digital forensics: Training Module 12 syllabus. .......... 117
Table 30: Template for planning the CSP Modules offering. .......... 135
Table 31: CyberSecPro general modules. .......... 143
Table 32: CyberSecPro health modules declaration. .......... 146
Table 33: CyberSecPro energy modules declaration. .......... 148
Table 34: CyberSecPro maritime modules declaration. .......... 149
Table 35: Categorisation of training offers in the 12 CSP modules: General. .......... 151
Table 36: Categorisation of training offers in the 12 CSP modules: Maritime. .......... 152
Table 37: Categorisation of training offers in the 12 CSP modules: Health. .......... 153
Table 38: Categorisation of training offers in the 12 CSP modules: Energy. .......... 154

# List of Acronyms

| | | |
|---|---|---|
| *2* | **2FA** | Two Factor Authentication |
| *A* | **ACM** | Association for Computing Machinery |
| | **AI** | Artificial Intelligence |
| | **AIA** | Artificial Intelligence Act |
| | **API** | Application Programming Interface |
| | **APT** | Advanced Persistent Threat |
| | **AR** | Augmented Reality |
| | **ARIA** | Accessible Rich Internet Applications |
| *C* | **CA** | Contract Agent |
| | **CC** | Creative Common |
| | **CC BY-NC-SA 4.0** | Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License |
| | **CCN** | Competence Centres Network, Cyber Competence Network |
| | **CCPA** | California Consumer Privacy Act |
| | **CDO** | Chief Data Officer |
| | **CE** | Computer Engineering |
| | **CERT** | Computer Emergency Response Team |
| | **CI** | Critical Infrastructures |
| | **CIA** | Confidentiality Integrity Availability |
| | **CISO** | Chief Information Security Officer |
| | **CISSP** | Certified Information Systems Security Professional |
| | **CMMC** | Cybersecurity Maturity Model Certification |
| | **CNI** | Critical National Infrastructure |
| | **CNN** | Convolutional Neural Network |

| | | |
|---|---|---|
| | **CoA** | Certificate of Attendance |
| | **COTS** | Commercial Off-the-shelf |
| | **CR** | Cyber Range |
| | **CS** | Computer Science |
| | **CSCL** | Computer-Supported Collaborative Learning |
| | **CSIRT** | Computer Security Incident Response Team |
| | **CSO** | Chief Security Officer |
| | **CSP** | Cloud Service Provider |
| | **CSR** | Corporate Social Responsibility |
| | **CSS** | Cascading Style Sheets |
| | **CTI** | Cyber Threat Intelligence |
| | **CVE** | Common Vulnerabilities and Exposures |
| | **CVSS** | Common Vulnerability Scoring System |
| | **CWE** | Common Weakness Enumeration |
| | **CyBoK** | Cyber Security Body of Knowledge |
| | **CyPR** | Cybersecurity Professional Register |
| *D* | **D** | Deliverable |
| | **DCM** | Dynamic Curriculum Management |
| | **DCMS** | Dynamic Curriculum Management System |
| | **DMZ** | Demilitarised Zone |
| | **DNS** | Domain Name System |
| | **DPIA** | Data Protection Impact Assessment |
| | **DTLS** | Datagram Transport Layer Security |
| *E* | **E2EE** | End-to-end encryption |
| | **EAP** | Extensible Authentication Protocol |

| | | |
|---|---|---|
| | **EC** | European Commission |
| | **E-CCS** | ECHO Cybersecurity Certification Scheme |
| | **ECHO** | European network of Cybersecurity centres and competence Hub for innovation and Operations |
| | **ECSF** | European Cybersecurity Skills Framework |
| | **ECTS** | European Credit Transfer and Accumulation System |
| | **EDR** | Endpoint Detection and Response |
| | **E-MAF** | ECHO Multi-Sector Assessment Framework (previously E-MSAF) |
| | **EMEA** | Europe, Middle East, and Africa |
| | **ENISA** | European Union Agency for Cybersecurity |
| | **EU** | European Union |
| *G* | **GDPR** | General Data Protection Regulation |
| | **GSM** | Global System for Mobile Communication |
| *H* | **HEIs** | Higher Education Institutions |
| | **HTML** | HyperText Markup Language |
| | **HTTPS** | Hypertext Transfer Protocol Secure |
| *I* | **ICTs** | Information and Communication Technologies |
| | **IDS** | Intrusion Detection System |
| | **IEEE** | Institute of Electrical and Electronics Engineers |
| | **IoT** | Internet of Things |
| | **IPR** | Intellectual Property Rights |
| | **IPS** | Intrusion Prevention System |
| | **ISO** | International Organization for Standardization |
| | **ISRM** | Information Security Risk Management |

| | | |
|---|---|---|
| | **IT** | Information Technology |
| *J* | **JAWS** | Job Access With Speech |
| *K* | **KA** | Knowledge Area |
| | **KPI** | Key Performance Indicator |
| | **KSA** | Knowledge, Skills, Abilities |
| | **KU** | Knowledge Unit |
| *L* | **LAN** | Local Area Network |
| | **LMS** | Learning Management System |
| | **LSTM** | Long Short-Term Memory |
| *M* | **MAN** | Metropolitan Area Network |
| | **MOOC** | Massive Open Online Courses |
| *N* | **NAT** | Network Address Translation |
| | **NIST** | National Institute of Standards and Technology |
| | **NVDA** | NonVisual Desktop Access |
| *O* | **OSI** | Open System Interconnection |
| | **OSINT** | Open-Source Intelligence |
| | **OT** | Operational Technology |
| *P* | **PC** | Project Coordinator |
| | **PETs** | Privacy Enhancing Techniques |
| | **PGP** | Pretty Good Privacy |

| | | |
|---|---|---|
| | **PPT** | Power Point Presentation |
| *Q* | **QUIC** | Quick UDP Internet Connections |
| *R* | **RBAC** | Role-Based Access Control |
| *S* | **SDLC** | Software Development Life Cycle |
| | **SDN** | Software-Defined Networks |
| | **SIEM** | Security Information and Event Management |
| | **SMIME** | Secure Multipurpose Internet Mail Extensions |
| | **SSH** | Secure Shell |
| *T* | **T** | Task |
| | **TCP** | Transmission Control Protocol |
| | **TCP/IP** | Transmission Control Protocol / Internet Protocol |
| | **TLS** | Transport Layer Security |
| | **ToC** | Table of Contents |
| *U* | **UDP** | User Datagram Protocol |
| *V* | **VLAN** | Virtual LAN |
| | **VPN** | Virtual Network Private |
| | **VR** | Virtual Reality |
| *W* | **WAN** | Wide Area Network |
| | **WCAG** | Web Content Accessibility Guidelines |
| | **WLAN** | Wireless LAN |

| | | |
|---|---|---|
| | **WMAN** | Wireless MAN |
| | **WP** | Work Package |
| | **WPA** | Wi-Fi Protected Access |
| | **WPA2** | Wi-Fi Protected Access 2 |
| *X* | **XSS** | Cross Site Scripting |

# Glossary of Terms

*C* **CSP competence**

The initial studies confirm the challenges of interpreting the knowledge areas, skills, and competencies differently across EU nations and organisations. Therefore, CSP D2.1 follows the guideline from the European Cybersecurity Skills Framework definition, “The ability to carry out managerial or technical activities and tasks on a cognitive or practical level; knowing how to do it.”

**CSP Dynamic Curriculum Management System (DCMS)**

Includes all the procedures and processes that CyberSecPro will use to manage the curriculum portfolio. The open-source learning platforms Moodle and/or e-class will be used (since the academic partners already use it in the academic programmes) for the CyberSecPro Dynamic Curriculum Management (DCM) integration. It will entail the entire curriculum creation, evaluation, review, approval, promotion processes, and regulation compliance (e.g., General Data Protection Regulation (GDPR)).

The main requirements of the CyberSecPro online DCM will be flexibility and responsiveness to the continuously changing needs of the cybersecurity market. The online DCM tool will be integrated by parametrising the Moodle or e-class open-source learning platform where the cybersecurity market needs will be monitored, and curricula will be managed.

**CSP Knowledge Areas (KAs)**

The Knowledge Areas (KAs) derived from D2.3 listed were based on the CyBoK Skills Framework, JRC recommendation and mainly from the European Cybersecurity Organisation report based on industry-academia cooperation and development work. However, the project will be further aligned with the ECSF and the market analyses' outcomes.

**CSP practical skill**

The initial studies confirmed the challenges of interpreting the knowledge areas, skills, and competencies differently across EU nations and organisations. Therefore, CSP D2.1 follows the guideline from the European Cybersecurity Skills Framework definition, “The demonstrated ability to apply knowledge, skills, and attitudes to achieve observable results”.

**CSP sector-specific training modules**

CSP training modules will concentrate on the health, maritime, and energy sectors. The modules will be shaped around real-life challenges in collaboration with the HEIs, companies and industries, adapting their content and approach to the specific knowledge areas and parametrizing the training tools and practical exercises accordingly.

**CSP syllabus**

All training modules are accompanied by a syllabus that include information like learning outcomes, who should attend, relative conventions and standards, prerequisite competencies (skills & knowledge), training module outline, list tools/access rights of tools, manuals, handbooks and handouts the delegates receive during the training, training tools that will be used, assessment methods, exams, study time (physical and online learning) and so on.

A standard template for a CSP syllabus is available in this deliverable and it will be used in all CSP training modules.

**CSP Trainees**

CSP Trainees refer to prospective IT professionals or individuals who enrol in CyberSecPro training programme.

**CSP Trainers**

CSP Trainers refer to CyberSecPro partners who provide training in each cybersecurity domain.

**CSP training format**

CSP training format describes the way how modules will be provided, i.e., “OnDemand,” “Web-based,” “Live Online,” “Live in Person,” “Hybrid/mix” etc.

**CSP training material**

Corresponds to all material that will be used by the educator/trainer to provide the CSP training module.

**CSP training modules**

Comprises courses, mini-courses, lectures, cyber hands-on exercises, cyber hackathons, cyber mornings & events, cybersecurity games, red/blue team exercises, summer schools, workshops, ad-hoc sector-specific seminars, on-demand mini-technological courses, and crisis management training.

**CSP training programme**

The programme consists of training modules that can be offered individually or as a package of modules; it will not lead to any certification, degree, or career paths; it will be used to enhance existing training offers to close the gaps between academic training supply and marketing professional demands.

**CSP training tools**

Training tools that will be used in the training of the CSP modules (the assessment of the various tools, selection and portfolio occurs in T2.3).

# 1 Introduction

## 1.1 Goals

This deliverable builds on the outcomes of CyberSecPro (CSP) deliverables D2.1, D2.2, and D2.3 of WP2, especially D2.3, which provided the structure, requirements, and specifications of the CyberSecPro education and training programme. The deliverable describes the 12 CSP core training modules derived from the deliverable D4.1, syllabi, key components of critical sectors, and Dynamic Curriculum Management (DCM) system. Following the DCM and programme specifications in D2.3, this deliverable outlines the main components and procedures of the CyberSecPro programme, focusing on the generic CyberSecPro training modules, templates, and key elements of the individual training modules specifically designed for the health, energy, and maritime sectors. The deliverable also details the enrolment procedures for the CyberSecPro programme and presents various templates and e-forms developed to facilitate the training process and offerings. These core training modules form the basis for developing specialised CSP modules for training cybersecurity professionals in the aforementioned CyberSecPro's critical sectors in deliverables D3.3-D3.5, respectively.

D2.3 prioritised cybersecurity knowledge areas and developed corresponding modules to address skill gaps in the cybersecurity workforce. D2.3 further described how the selection of modules was carried out by evaluating course offerings from CyberSecPro partners, ensuring alignment with prioritised knowledge areas and avoiding duplication of effort. The selected modules are intended to bridge skill gaps, cater to market-oriented capabilities, and align with the European Cyber Security Framework (ECSF). The 12 core cybersecurity training modules form the foundation for the CyberSecPro curricula and syllabi.

Furthermore, this deliverable delves into the intricate details of the CyberSecPro programme, outlining its main components and procedures. The deliverable is structured to offer a guideline and tool as well as provides a clear and comprehensive understanding of the CyberSecPro programme's main components and procedures. The subsequent sections provide in-depth details of each aspect of the programme, ensuring that training providers are fully equipped to utilise valuable training guidelines and resources based on the innovation work conducted in CyberSecPro. This deliverable comprises the content that contributes towards the project goals, namely:

- **Addressing the Cybersecurity Skills Gap with CyberSecPro Training Modules**: The CyberSecPro training programme comprises a comprehensive suite of 12 generic training modules, each designed to equip participants with the knowledge and skills essential to succeed in the ever-evolving cybersecurity landscape. These modules cover a broad spectrum of cybersecurity topics, ranging from cybersecurity essentials and management to emerging technologies and critical infrastructure security.
- **Generic CyberSecPro Training Modules and Syllabi**: The 12 generic training modules of the CyberSecPro programme provide a solid foundation in cybersecurity principles and practices. These modules cover fundamental concepts such as cybersecurity risk management, software security, network security, data protection, privacy technologies, cyber threat intelligence, and penetration testing.
- **Domain-Specific Training Modules and Key Elements - Tailored to the Needs of the Critical Sectors Health, Energy, and Maritime**: In addition to the generic modules, the CyberSecPro model syllabus and programme offers foundation for the sector-specific training modules. The deliverables D3.3, D3.4, and D3.5 are tailored to the unique cybersecurity challenges and opportunities faced by the health, energy, and maritime domain. These modules provide participants with in-depth knowledge of the specific cybersecurity threats, vulnerabilities, and mitigation strategies relevant to their respective sectors.
- **Ensuring Consistency and Quality with CyberSecPro Training Module Templates**: A set of comprehensive training module templates has been developed to ensure consistency and quality across the entire CyberSecPro programme. These templates provide a structured

framework for developing and delivering each training module, covering key elements such as target audience, learning objectives, syllabus, content outline, teaching methods, assessment strategies, and resources.

- **Streamlining the Participation Process with Enrolment Procedures**: The CyberSecPro programme has established clear and streamlined enrolment procedures to facilitate participation for qualified individuals. These procedures include eligibility criteria, application process, selection criteria, and admission requirements and will be facilitated by the Dynamic Curriculum Management (DCM) System.
- **Enhancing Training Providers' Efficiency and Organisation with Templates and e-Forms**: A variety of templates and e-forms have been developed to streamline the administrative processes associated with the CyberSecPro programme. These include curricula, teaching materials, exercises, trainees' background and topic request forms, and registration forms.
- **Ensuring Relevance and Adaptability with Dynamic Curriculum Management (DCM)**: The CyberSecPro programme utilises a DCM system to ensure the training content remains relevant and up to date with the evolving cybersecurity landscape. The DCM system continuously monitors cybersecurity market trends, identifies emerging threats and vulnerabilities, and incorporates new knowledge and technologies into the training modules. A detailed information about DCM is provided in D2.3.

The CyberSecPro programme's main component and procedure deliverables outline the generic CSP training modules syllabus, robust templates, streamlined procedures, and DCM system. The following part of the report provides comprehensive details of these components in subsequent sections and subsections.

## 1.2 Methodology

Within the framework of D3.1, the methodology adopted is presented with the purpose of generating the exact CSP programme consisting of various types of modules (e.g., seminars, courses, exercises) developed by collaborating partners.

### 1.2.1 Criteria setting

The CSP programme's main characteristics were set to be:

- **Simple and Consistent**: Covering the 10 knowledge areas needed by the market (as described in deliverables D2.1, D2.3, D4.1).
- **Enriched**: Based on the partners (i.e., CSP training providers) and utilising their long experience in cybersecurity training (as described in deliverables D2.2, D4.1), the CSP programme will be further enriched since it will be based on the collective cybersecurity intelligence of the partners.
- **Unified**: Despite the fact that partners use different titles for their training modules (see D2.2, D4.1), consensus was reached to homogenise the titles of the generic CSP modules.
- **Collaborative**: The CSP programme will offer joint training modules and syllabus to enable mobility among the CSP training providers.
- **Dynamic**: The CSP programme will be agile in terms of further participation of partners in the development and operation of the programme and in terms of developing new seminars, training offers, and updated course materials.

### 1.2.2 Process followed

The process followed to generate the final CSP programme consists of two phases, described in the following subsections.

#### 1.2.2.1 Phase 1: Modules Declaration Phase.

In this phase, the steps followed are:

**Step 1:** Partners declared all modules/titles that are already in use, and they are willing to offer in the ten knowledge areas in D4.1.

**Step 2:** Partners requested to list the specific modules/used titles (as declared in step 1) in four categories (general, maritime, health, and energy) under the 12 CSP modules categories. A complete procedure for declaring modules by every partner involved is given in the tables titled 'General/Maritime/Health/Energy Module Declaration' in Annex A. This comprehensive documentation is designed to ensure transparency and facilitate a seamless collaboration process among all partners.

The aim is to ensure a comprehensive and organised allocation of resources and expertise across all 12 CSP modules, facilitating effective collaboration and knowledge sharing.

#### 1.2.2.2 Phase 2: Finalising CSP Programme

This phase involves the following steps:

**Step 1:** Module Title Analysis and Comparison

- The titles of the modules submitted by each partner in Annex A [4] were analysed and compared against existing frameworks and common practices, such as e-CF [20], ECSF [5], CyBoK [14], and the JRC taxonomy [26].

**Step 2:** Determining the CSP Programme Structure

- Based on the analysis, a final proposal for the CSP programme structure was developed, with common titles and types of modules.

**Step 3:** Identifying Lead Partners

- Specific partners were identified to take the lead in developing each module.

**Step 4:** Supporting Partner Collaboration

- Lead partners will also support other partners in designing the syllabus and training materials for the sector-specific modules.

**Step 5:** Designing Comprehensive Training Modules

- Syllabi for the 12 CSP modules (D3.1) were designed to create complete training modules (similar to an academic course), which will serve as the basis for the sector-specific syllabus and training materials.

**Step 6:** Announcing Training Module Offerings

- The sector-specific training modules will be announced as subsets of the corresponding generic syllabus for the 12 modules. It is worth noting, the sector-specific training modules would include both the general and sector-specific part within the training module syllabi.
- Consider the factors listed in the following section titled Dynamic Nature of the CSP Programme.

The finalisation done based on WP2 development work of CSP in adding to comprehensive EU based studies referred and listed [5-25] in this report. For a detailed overview of these arrangements, please refer to the Final CSP Programme’s table in Annex B.

Annex F presents those **cybersecurity academic programs/courses** which have been reviewed/complemented/enhanced with **new CSP modules** during the WP3 (tasks T3.4, T3.5, and T3.6).

### 1.2.3 Dynamic Nature of the CSP programme

All partners in the CSP project are cordially invited to participate in the sector-specific modules recognising the valuable contributions they could bring. This invitation considers their unique capabilities and the amount of effort, measured in person-months, they could potentially dedicate to this project. It is essential to note:

- The CSP training offering will consider the capabilities of CSP training providers and ensure the modules are adoptable and realistic based on their resources.
- Therefore, the final syllabi will be customised to accommodate the practicalities, resources, and practices of each provider.

Furthermore, it needs to be acknowledged that some partners have generously offered their support in developing training materials for these sector-specific modules. We believe that all partners' combined expertise and resources will significantly enrich the development and effectiveness of the CSP training modules. This continuous involvement of partners and the development of modules and seminars underlines the dynamic nature of the CSP programme and allows the programme to grow and adapt to the current requirements in the sectors covered therein.

Regarding the ECTS element, the WP3 propose and built new cybersecurity training modules focusing on the sectors of maritime, health, and energy. In detail, a set of 72 training modules (generic and sector-specific) has been designed. The employed training model is focused to the needs of adult learners, it is aligned with the objectives of training providers to provide courses equipped with micro-credentials addressing market real needs by bridging the gap between education / training and work. This employed training model is based on the principle of learning outcomes so as to exploit effectively and efficiently related EU tools (e.g. ECTS, ECVET, EQF, Europass, etc.). Regarding the ECTS adoption, an in-depth study has been included in the task T3.3 (deliverable D3.2; Section 3.3) which sheds light on the credits in training programs'issue. According to the latest of the EU documents , , and especially the QUATRA – TPG A Working Group on Micro-credentials (Q4 of 2023) guidelines and recommendations , the micro-credentials adoption and their ECTS mapping are still missing from the agendas of the EU National Education Authorities, the Higher Education Institutes, and the Quality Assurance Agencies. Nevertheless, the CSP project has proposed a novel and formulated path to calculate the micro-credentials' volume on each CSP module and on any professional training module outside the scope of this project. It must be noted that the micro-credentials volume has been announced on the DCM platform regarding each training module which has been designed during the tasks T3.4, T3.5, and T3.6.

Similarly, tangible benefits to participants—such as ECTS credits, certificates, badges, and the status of each module (whether it is new, updated, or already offered by partner universities)—will be specified in each training programme individually. These aspects are dynamic and tailored to specific contexts and will be detailed in upcoming versions of CSP deliverables.

# 2 CyberSecPro Programme and Value Proposition

Based on the cybersecurity market demand and supply analysis outcomes in D2.1 and D2.3, CyberSecPro programme aims to offer state-of-the-art training modules considering market demand and CSP partners' supply of training offerings. The approach is helping to fill the gaps in the European cybersecurity workforce and consolidating EU cybersecurity posture and competitiveness. The core training modules of the CyberSecPro programme are outlined as follows.

- Module 1 - Cybersecurity Essentials and Management
- Module 2 - Human Factors and Cybersecurity
- Module 3 - Cybersecurity Risk Management and Governance
- Module 4 - Network Security
- Module 5 - Data Protection and Privacy Technologies
- Module 6 - Cyber Threat Intelligence
- Module 7 - Cybersecurity in Emerging Technologies
- Module 8 - Critical Infrastructure Security
- Module 9 - Software Security
- Module 10 - Penetration Testing
- Module 11 - Cyber Ranges and Operations
- Module 12 - Digital Forensics

The identified CSP training modules cover most of the European cybersecurity market's demanded workforce with hands-on knowledge, skills and competencies. CSP studies confirm that some of the sought-after buzzwords are not covered in the CSP training module naming conventions (see above 12 CSP training modules). However, the content is covered within the CSP training module syllabus. For example, cybersecurity for emerging technology, artificial intelligence and cybersecurity tools and technologies are already covered in CSP training module syllabus within relevant CSP modules.

## 2.1 Who Should Take CyberSecPro Training?

The training delivered through the CSP targets the professionals who would like to develop their skills (skilling / re-skilling) on the topics identified under the 12 CSP training modules. These professionals, no matter if they are in the initial steps of their career or at a later stage, would like to become competent enough to manage the upcoming challenges in their areas of interest, especially emerging (in terms of cybersecurity) in the sectors of healthcare, energy and maritime. Overall, CSP course modules are designed for individuals with some experience or interest in cybersecurity and aim to enhance their skills, knowledge, and capabilities in the field. The target audience may include:

1. **IT Professionals**: Those already working in IT roles, such as system administrators, network administrators, or IT support staff, who want to specialize in cybersecurity.
2. **Security Analysts**: Individuals involved in analysing and responding to security incidents or monitoring and assessing the security status of an organisation.
3. **System Administrators and Network Engineers**: Professionals responsible for managing and securing IT systems, networks, and infrastructure.
4. **Developers**: Software developers interested in secure coding practices and understanding how to build more secure applications.
5. **IT Managers and Executives**: Managers and executives responsible for overseeing IT operations and making strategic decisions related to cybersecurity within an organisation.
6. **Risk Management Professionals**: Individuals involved in assessing and managing cybersecurity risks within an organisation.
7. **Law Enforcement and Government Personnel**: Those working in roles related to cybersecurity in law enforcement, government agencies, or defence.

8. **Ethical Hackers and Penetration Testers**: Professionals interested in learning advanced techniques for identifying and mitigating security vulnerabilities through ethical hacking and penetration testing.
9. **Cybersecurity Enthusiasts**: Individuals who may not have a formal background in IT but have a strong interest in cybersecurity and want to build their skills.
10. **Recent Graduates**: College or university graduates with a degree in computer science, information technology, or a related field who want to specialize in cybersecurity.

## 2.2 When Should You Take CyberSecPro Training?

The timing for taking the CSP professional training depends on various factors, namely, the current career stage, the goals, and the interest in the specific content of each module. Below, some scenarios are listed that might be appropriate to consider when entering the CSP training:

1. **Start of Career**: If an individual begins their career in IT or cybersecurity, the CSP basic training will provide them with the essential skills and knowledge in the field.
2. **Career Transition**: If the individual professional is transitioning from another IT role to a cybersecurity-related role, the CSP training will help to acquire the specialised digital skills required for the new position.
3. **Skill Gap Identification**: If the individual professional identifies specific cybersecurity-related skill gaps, the CSP training will help them address them and become more competent.
4. **Change of Job**: If the individual professional moves into an advanced role with more cybersecurity responsibilities or transitions to a specialised area within cybersecurity (e.g., penetration testing, incident response), the CSP training will support them in confronting the new challenges.
5. **Preparation for Certifications**: The CSP training will support the individual professional to obtain industry-recognised certifications in cybersecurity.
6. **Organisational Training Initiatives**: Sometimes, employers invest in the professional development of their employees by providing cybersecurity training. CSP may consist of a well-justified alternative based on the state-of-the-art, addressing actual needs.
7. **Keeping Up to date with Industry Trends**: Given the rapidly evolving nature of cybersecurity, staying up to date with the latest threats, technologies, and best practices is crucial. The CSP training will help the individual professional to stay updated with the cybersecurity industry developments.
8. **Post-incident or Audit**: If an organisation has experienced a security incident or is preparing for an audit, the CSP training will enhance the individual professional’s capabilities and ensure compliance with security standards.
9. **Self-assessment**: If the individual professional self-assesses their cybersecurity knowledge and skills and finds areas that require improvement or updating, the CSP training will be a strategic move to gain this improvement.
10. **Continuous Learning**: Cybersecurity is a field that requires continuous learning. Regularly taking training courses will help the individual professional stay sharp, adapt to emerging threats, and remain competitive in the job market.

Before enrolling in the CSP training modules, the individual needs to assess their current skills, identify goals, and choose the modules that align better with their objectives. Additionally, the individual needs to consider the prerequisites and recommended experience levels for each module to ensure that they match their current proficiency in cybersecurity.

## 2.3 Why You Need CyberSecPro Training?

CSP training modules cover state-of-the-art cybersecurity training, covering actual market needs in the maritime, health, and energy sectors and beyond; the identified modules resulted from a thorough requirements analysis between various types of stakeholders. Individuals who manage to follow all the 12 CSP training modules successfully will be able to operate as cybersecurity professionals, supporting organisations to confront various challenges, including their protection against cyber threats, the defence against evolving threats, the prevention of cybersecurity breaches, the compliance with regulations, the incident response and recovery, and many other.

The goals of the individual professionals participating in the CSP modules may vary according to their background, career objectives, and the specific focus of the modules. However, the common goals for the target audience may include the following:

1. **Skill Enhancement**: Participants aim to enhance their technical skills in areas identified under the CSP module areas.
2. **Knowledge Expansion**: Professionals may seek to deepen their understanding of the latest trends, tools, and technologies in the rapidly evolving field of cybersecurity.
3. **Certification Preparation**: Many professionals take cybersecurity courses to prepare for industry-recognized certifications and improve their career prospects.
4. **Career Advancement**: Individuals may enrol in professional development courses to improve their opportunities for career advancement, either within their current organisation or when seeking new opportunities in the job market.
5. **Stay up to date with Threat Landscape**: Given the dynamic nature of cybersecurity threats, professionals aim to stay up to date with the latest tactics, techniques, and procedures cyber attackers employ to better defend their organisations.
6. **Risk Management Skills Development**: For those involved in risk management, their interest is to develop a strong understanding of risk assessment methodologies and strategies for mitigating cybersecurity risks.
7. **Ethical Hacking and Penetration Testing Expertise**: Individuals interested in ethical hacking and penetration testing seek to develop the skills to identify and address vulnerabilities in systems and networks.
8. **Policy and Compliance Knowledge Expansion**: Professionals working in compliance or policy roles may take courses to understand the legal and regulatory frameworks surrounding cybersecurity, ensuring their organisation's adherence to standards.
9. **Security Awareness and Education Enhancement**: Some professionals may focus on developing skills related to educating others within their organisation about cybersecurity best practices and fostering a security-aware culture.
10. **Adaptability to Emerging Technologies**: With the proliferation of new technologies, professionals aim to develop the adaptability and knowledge necessary to secure emerging technologies such as cloud computing, Internet of Things (IoT), and Artificial Intelligence (AI).

By achieving these goals, cybersecurity professionals can contribute to the overall security presence of their organisations and stay competitive in a field that demands continuous learning and adaptation.

## 2.4 Prerequisites and Requirements for Taking CyberSecPro Training

The prerequisites for taking CSP training establish a baseline understanding of Information and Communication Technologies (ICTs) and digital frameworks, ensuring participants have a solid foundation to build upon during the training (Figure 1). Without this basic knowledge, individuals may struggle to comprehend the more complex cybersecurity concepts and techniques the programme teaches. Therefore, each training module defines the prerequisite competencies (skills and knowledge) required to take the module (e.g., modules that learners must have attended before to understand the course).

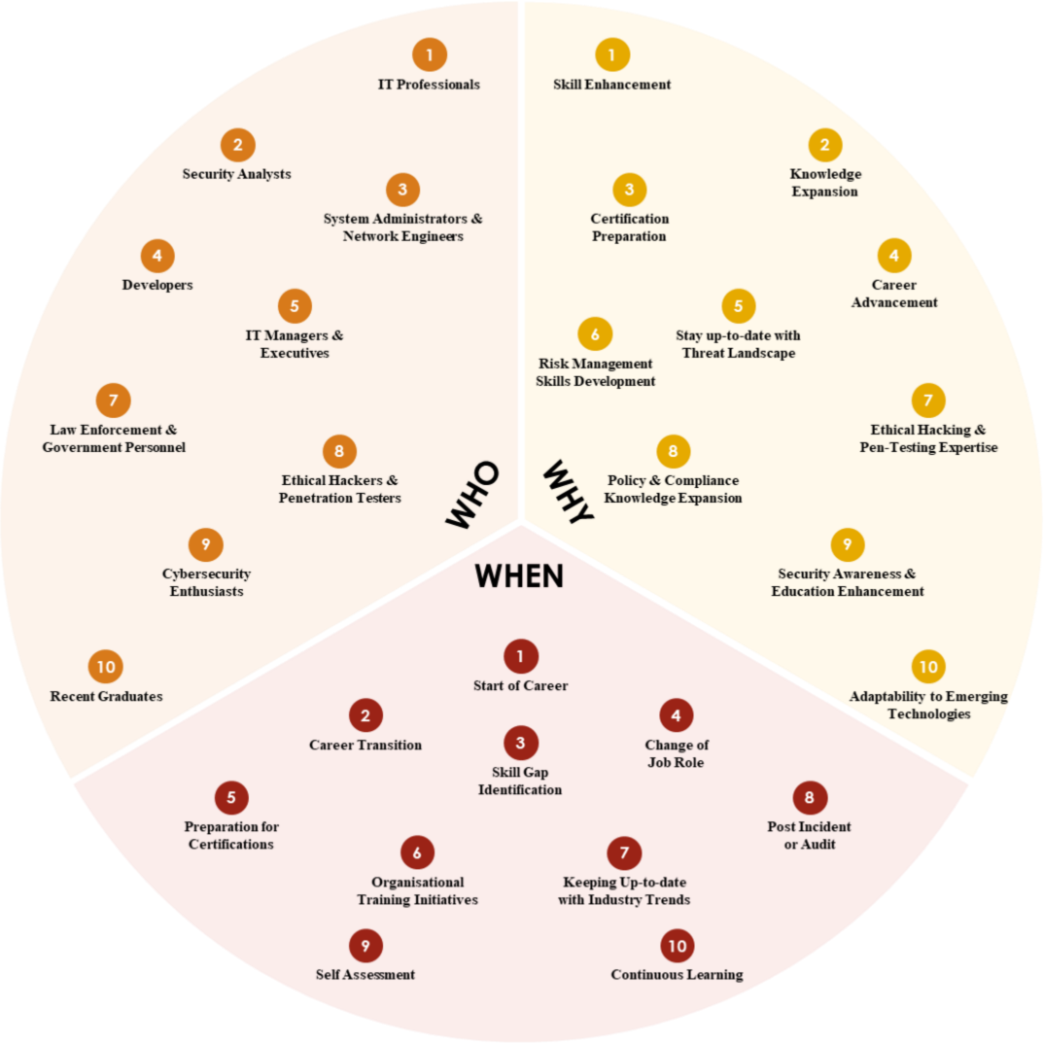

WHO
1 IT Professionals
2 Security Analysts
3 System Administrators & Network Engineers
4 Developers
5 IT Managers & Executives
7 Law Enforcement & Government Personnel
8 Ethical Hackers & Penetration Testers
9 Cybersecurity Enthusiasts
10 Recent Graduates
WHY
1 Skill Enhancement
2 Knowledge Expansion
3 Certification Preparation
4 Career Advancement
5 Stay up-to-date with Threat Landscape
6 Risk Management Skills Development
7 Ethical Hacking & Pen-Testing Expertise
8 Policy & Compliance Knowledge Expansion
9 Security Awareness & Education Enhancement
10 Adaptability to Emerging Technologies
WHEN
1 Start of Career
2 Career Transition
3 Skill Gap Identification
4 Change of Job Role
5 Preparation for Certifications
6 Organisational Training Initiatives
7 Keeping Up-to-date with Industry Trends
8 Post Incident or Audit
9 Self Assessment
10 Continuous Learning

Figure 1: Schematic overview on the value proposition for the CyberSecPro programme.

## 2.5 Pedagogical Aspects

In order to enhance the quality of the selected education and training modules, specific pedagogic approaches have been identified in CyberSecPro Deliverable D2.3 CyberSecPro Programme Specifications under section 3.4. The general guidelines from D2.3 holds vital significance for the CyberSecPro education and training programme. CyberSecPro consider the recommended scientific pedagogical understanding from D2.3, however, this section focuses on design aspect, and thus presenting practical pedagogical aspects to help offering the CyberSecPro training modules in practice. Table 1 presents some suggestions of the pedagogical best-practices based on different delivery mode and methods.

Table 1: CyberSecPro recommended training delivery method.

| Format | Suggested training delivery methods |
|---|---|
| Short & Flexible formats | **Ad-hoc seminars, fast courses, lunch & learn:**<br>• Focus on specific topics and actionable takeaways.<br>• Use case studies, real-world examples, and practical demonstrations. |

| Format | Suggested training delivery methods |
|---|---|
| | • Encourage active participation through Q&A, polls, and breakout groups.<br>• Keep content concise and engaging, using multimedia elements. |
| | **Summer schools, workshops:**<br>• Combine lectures with hands-on exercises and group projects.<br>• Invite subject matter experts for guest talks and discussions.<br>• Offer opportunities for networking and collaboration.<br>• Consider offering different tracks for varying skill levels. |
| | **On-demand mini technological courses:**<br>• Micro-learning modules with bite-sized content.<br>• Interactive learning experience with quizzes, simulations, and gamification.<br>• Offer self-paced learning options with flexible schedules.<br>• Provide clear learning objectives and performance assessments |
| Hands-on & Experiential formats | **Lorem ipsum Cyber exercises, hackathons, cyber games:**<br>• Simulate real-world scenarios with realistic challenges.<br>• Encourage collaboration, problem-solving, and critical thinking.<br>• Provide immediate feedback and performance analysis.<br>• Integrate debriefing sessions to learn from mistakes and share best practices. |
| | **Red/blue team exercises:**<br>• Focus on vulnerability assessments and penetration testing.<br>• Promote adversarial thinking and ethical hacking skills.<br>• Create a safe environment for experimentation and learning.<br>• Include post-exercise reports and improvement recommendations. |
| | **Cyber hands-on exercises:**<br>• Provide practical tasks on specific tools and techniques.<br>• Offer guided guidance with step-by-step instructions.<br>• Allow for troubleshooting and experimentation.<br>• Incorporate performance evaluations and feedback. |
| Broader & Immersive formats | **Summer schools, workshops, ad-hoc sector specific seminars:**<br>• Combine lectures, workshops, and case studies.<br>• Invite industry experts and practitioners for guest sessions. |

| Format | Suggested training delivery methods |
|---|---|
| | • Offer opportunities for networking and community building.<br>• Tailor content to specific industry sectors and challenges. |
| | **Academic campus courses:**<br>• Integrate theoretical knowledge with practical applications.<br>• Use project-based learning and research opportunities.<br>• Encourage critical thinking and ethical considerations.<br>• Offer diverse assessment methods like presentations, reports, and exams. |
| | **Crisis management training:**<br>• Focus on decision-making in stressful situations.<br>• Use scenario-based simulations and role-playing exercises.<br>• Develop communication and leadership skills.<br>• Evaluate team performance and identify improvement areas. |

## 2.6 Soft and Transversal Skills

CyberSecPro studies and outcomes in D2.1 and D2.3 highly recommending a horizontal soft skill for the cybersecurity professionals. Many studies including CyberSecPro confirms the soft skills are essentials for cybersecurity working-life practices [1-4] [27-29]. Many researchers argues that soft skills are not only soft skills but needed transversal and transferable skills. Rathod and Kämppi (2023) study found that beyond cybersecurity technical expertise, success hinges on soft skills like communication, teamwork, and problem-solving [30]. Yet, these crucial abilities often receive less attention in training programmes. They are experimenting the approach for the cybersecurity students in higher education since many years and their study found best practices that elevate training by integrating essential soft skills.

- **Weave the Thread**: Identify key soft skills relevant to your field and seamlessly integrate them into your existing learning objectives and activities. Imagine projects requiring collaborative problem-solving or presentations honing communication skills. Real-world scenarios further solidify connections.
- **Bridge the Gap**: Showcase how soft skills amplify the impact of technical expertise. Explain how clear communication translates complex ideas, or how teamwork tackles intricate projects. Design activities demanding both technical mastery and soft skills application.
- **Career Connection**: Highlight the real-world value of soft skills across diverse industries. Invite industry professionals to share their experiences, and help learners map these skills to their career aspirations. Integrate activities like self-reflection and goal setting, emphasizing the crucial role of soft skills in career navigation.
- **Assess with Insight**: Develop clear assessment criteria to evaluate soft skills growth. Utilize diverse methods like peer feedback, observation, presentations, and case studies. Provide ongoing feedback and opportunities for improvement, fostering a growth mindset.
- **Embrace the Advantage**: Create a supportive learning environment where experimentation and feedback are encouraged. Offer self-directed learning opportunities and leverage technology tools. Regularly review and adapt your approach based on feedback and learner needs.

Soft skills are not secondary; they are essential tools for cybersecurity professional success. The CSP training modules aiming to integrate them throughout training and empower learners to not only master cybersecurity technical skills but also navigate the complexities of cybersecurity field with confidence and adaptability. Teaching soft, transversal, and transferable skills requires a different approach compared to technical skills. These skills often require practice, reflection, and feedback in real-world scenarios. Table 2 presents some key approaches to consider.

Table 2: CyberSecPro recommended soft skills development practices.

| Title | Title |
|---|---|
| Experiential Learning | • Case studies, role-playing, simulations: Place learners in situations where they can practice and apply the skills in a safe environment.<br>• Group projects, collaborative tasks: Encourage teamwork, communication, and problem-solving through collaborative activities.<br>• Real-world challenges, internships, volunteering: Provide opportunities to apply skills in authentic contexts.<br>• Hackathons, gamified learning: Use game-based elements to increase engagement and motivation. |
| Reflection and Feedback | • Self-reflection exercises, journaling: Encourage learners to reflect on their experiences and identify areas for improvement.<br>• Peer feedback, group discussions: Provide opportunities for learners to receive feedback from others and learn from each other's experiences.<br>• Coaching, mentoring: Offer personalized guidance and support to help learners develop specific skills.<br>• 360-degree feedback: Provide feedback from different perspectives, including peers, instructors, and supervisors. |
| Scaffolding and Differentiation | • Start with basic skills and gradually increase complexity.<br>• Offer tiered activities and resources to cater to different learning styles and levels.<br>• Provide clear instructions, rubrics, and expectations for success.<br>• Offer individual support and guidance to learners who need it. |
| Technology-Enhanced Learning | • Virtual reality (VR) and augmented reality (AR): Immerse learners in realistic scenarios for practicing skills.<br>• Collaborative online platforms: Facilitate communication, feedback, and group work.<br>• Mobile learning apps: Provide on-the-go access to learning resources and activities.<br>• Simulations and games: Offer interactive experiences to learn and practice skills. |
| Integration into Curriculum and Training | • Treat soft skills as an essential topic; integrate them throughout training programmes.<br>• Connect them to technical skills and course content. |

| Title | Title |
|---|---|
| | • Show learners how these skills are relevant to their future careers.<br>• Develop assessment methods that measure soft skills development. |

# 3 CyberSecPro Generic Training Modules Syllabus

The CyberSecPro Generic Training Modules Syllabus provides a comprehensive overview of the **12 core new CSP training modules** that form the foundation of the CyberSecPro programme. These modules cover a broad spectrum of cybersecurity topics, from essential cybersecurity principles to advanced penetration testing techniques. The syllabus for each module includes detailed information on the target audience, learning objectives, prerequisites, course structure, teaching methods, assessment methods, and recommended learning resources. This syllabus is designed as a generic model and a template that can be adapted to meet the specific needs of different organisations and learners. It serves as a metadata repository, guiding the development of customised cybersecurity training programmes and helping to identify individual training needs in the three envisaged CSP domains - Energy, Health, and Maritime. The modules can be delivered in various formats, including instructor-led, online, and blended learning approaches such as general academic courses, professional training, workshops, cyber exercise sessions, sector-specific seminars, hackathons, and interactive cybersecurity labs.

It is important to note that the syllabus does not include specific details such as offering dates, module enrolment processes, or other important dates. The purpose of this document is to provide a foundational framework rather than dynamic logistical information. Such details are highly variable and subject to change; therefore, they will be provided within each specific training programmes and communicated through the DCM platform. The DCM serves as the instantiation of the syllabus in the different training programmes, housing up-to-date content and logistical information.

Similarly, tangible benefits to participants—such as ECTS credits, certificates, badges, and the status of each module (whether it is new, updated, or already offered by partner universities)—will be specified in each training programme individually. These aspects are dynamic and tailored to specific contexts and will be detailed in upcoming versions of CyberSecPro deliverables, not within D3.1.

The following subsections provides the detailed syllabus for each CSP training module, starting from the Cybersecurity Essentials and Management to Digital Forensics. The syllabus also provides the foundation for tailoring the modules to address the unique cybersecurity challenges of the critical sectors in subsequent deliverables in CSP project. The syllabus can guide the development of customised cybersecurity training programmes and identify individual training needs. The syllabus is also a valuable tool for cybersecurity educators, providing a comprehensive framework for designing and delivering effective cybersecurity training courses. The CyberSecPro Generic Training Modules Syllabus is a valuable resource for anyone interested in developing their cybersecurity professional education and training.

It is necessary to state that CyberSecPro's early deliverables, D2.1 and D2.2, identified horizontal skills relevant to all CSP training modules. These skills, also known as soft or professional skills, may be identified under broad categories: communication, problem-solving, critical thinking, teamwork, leadership, resilience, adaptability, writing, time management, organisation, interpersonal skills, and ethics, among others. Soft skills are crucial in today's dynamic and interconnected world and can be a fulcrum of personal and professional cybersecurity career success. The importance and applicability of these professional skills in CSP training modules cannot be overemphasised. However, these horizontal skills, which are not unique to any CSP training module, are not explicitly provided as part of each syllabus description to avoid redundancy. They have only been described as part of the first core module syllabus (see soft/professional skills in section 3.1.3).

## 3.1 Module 1 - Cybersecurity Essentials and Management

### 3.1.1 Target Audience and Goals

This CSP training module is designed for individuals who are:

- IT professionals responsible for managing and securing information systems.
- Security professionals responsible for protecting organisations from cyberattacks.

- Business leaders who need to understand the risks and costs of cyberattacks.

**Goals:**

The goal of the Cybersecurity Essentials and Management is to equip participants, particularly managers or beginners in technical cybersecurity, with the foundational knowledge and skills necessary to create a strategy to protect critical systems and data.

**Following are breakdown of the key goals:**

- Provide a comprehensive overview of essential cybersecurity concepts and principles: This includes understanding the fundamentals of cybersecurity, the different types of threats and vulnerabilities, and the basic controls in place to mitigate them.
- Equip participants with the knowledge and skills to build a cybersecurity strategy: This involves learning how to identify and assess risks, prioritize vulnerabilities, and implement appropriate controls.
- Develop foundational skills in key areas: This includes understanding the cybersecurity body of knowledge, ethical and professional practices, and soft skills needed for teamwork.

Overall, the training aims to empower participants to take an active role in protecting their organisation's critical systems and data. To acquire practical knowledge and skills in all cybersecurity domains that forms the foundation for further training in various cybersecurity disciplines.

### 3.1.2 Description of Training Module 1: Cybersecurity Essentials and Management

Table 3: Cybersecurity essentials and management: Training Module 1 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | **CSP001** |
| **Content** | **Module title**<br>*The Title of the training module* | **Cybersecurity Essentials and Management** |
| | **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Cybersecurity Essentials<br>• Cybersecurity Management<br>• Cybersecurity for the Modern Workplace- Cybersecurity Essentials and Principles<br>• A Comprehensive Overview of Cybersecurity Core Concepts<br>• Mastering the Fundamentals of Cybersecurity |

| | | |
|---|---|---|
| | | • From Essentials to Management: Cybersecurity for Managers and Leaders<br>• Essential Cybersecurity Skills for Managers and Leaders<br>• Introduction to Information and Cybersecurity<br>• Introduction to Information Security Management<br>• Management of Information Security |
| | **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module overview**<br>*High-level module overview* | This training module provides a foundational understanding of cybersecurity essentials and management principles, equipping participants with the knowledge and skills to manage information and cybersecurity in an organisation. |
| | **Module description**<br>*Indicates the main purpose and description of the module.* | The Cybersecurity Essential and Management training module provides trainees with the knowledge of basic concepts and skills necessary to manage the security of information assets in an organisation. The module covers a wide range of topics as provided under the "Main topics and content list." The module is designed to be more practical and hands-on and allows participants to gain experience in applying the concepts they learn through a variety of exercises and activities. |
| | **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance* | Mainly KA1<br>Minor content matches with others including KA2, KA3, KA4, KA7 |

| | | |
|---|---|---|
| | *KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | |
| | **Category(s) of capabilities**<br>*Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | Refer and check D4.1. |
| | **Learning outcomes and targets**<br>*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, participants will gain the following:<br>**Knowledge:**<br>• Ethical principles and guidelines for cybersecurity professionals.<br>• Basic cybersecurity terminology and concepts<br>• The CIA triad (confidentiality, integrity, and availability).<br>• Types of cybersecurity threats and vulnerabilities.<br>• Cybersecurity frameworks and models (ISO/IEC 27001, ECSF, NIST Cybersecurity Framework, CyBoK).<br>• Human psychology in cybersecurity.<br>• Secure architecture design and implementation principles.<br>• Data security and privacy principles.<br>• Cybersecurity governance practices and frameworks.<br>• Cybersecurity laws, regulations, and legislation.<br>• Information security risk management (ISRM) methodologies.<br>**Skills:**<br>• Identify and classify cybersecurity threats and vulnerabilities.<br>• Conduct vulnerability assessments and penetration tests. |

| | | |
|---|---|---|
| | | • Implement vulnerability management strategies.<br>• Develop and implement cybersecurity policies and procedures.<br>• Select and implement security controls.<br>• Design secure network architectures and systems.<br>• Implement data security measures.<br>• Manage user access and privileges.<br>• Communicate cybersecurity risks effectively.<br>• Document cybersecurity incidents and procedures.<br>• Conduct self-assessments and stay updated on cybersecurity trends.<br>**Competencies:**<br>• Apply ethical decision-making in cybersecurity situations.<br>• Analyse the impact of cybersecurity threats and vulnerabilities.<br>• Design and implement secure solutions.<br>• Manage and mitigate cybersecurity risks.<br>• Educate and empower users on cybersecurity best practices.<br>• Collaborate effectively with stakeholders on cybersecurity initiatives.<br>• Adapt to changing cybersecurity threats and technologies.<br>• Embrace continuous learning and professional development. |
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Ethical Conduct and Professionalism<br>• Foundational Knowledge of Cybersecurity<br>• Cybersecurity Body of Knowledge<br>• Threats and vulnerabilities<br>• Human Factor Considerations |

| | | |
|---|---|---|
| | | • Secure Architecture Design and Implementation<br>• Security Controls Selection and Implementation<br>• Data Security and Privacy by Design<br>• Cybersecurity Governance: Policies, Procedures, Standards, Methodologies and Frameworks<br>• Cybersecurity Governance: Cybersecurity related Laws, Regulations and Legislations including Auditing, Legal and Ethical Compliance<br>• Information and Cyber Security Risk Management (ISRM)<br>• Soft Skills and Leadership Development<br>• Effective Communication and Documentation<br>• Self-Reflection and Continuous Learning |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Management/ Logistics** | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the* | Check online in CyberSecPro DCM System for current information on the specific module |

| | | |
|---|---|---|
| | *location. If virtual, provide the URL link of the website.* | instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Basic IT training (or) EU Digital Competence (DigComp) Framework level know-how |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | Mainly ECSF Profile 1: Chief Information Security Officer (CISO)<br>Minor content matches with other ECSF profiles. |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | *Check online in CyberSecPro DCM System for current information on the specific module instantiation. Some of the aspects considered are listed below:*<br>**Knowledge-based assessments**: These assessments measure the participant's knowledge of the material covered in the training. They can be administered in various |

| | | |
|---|---|---|
| | | ways, such as through multiple-choice, essay, or fill-in-the-blank questions.<br>**Performance-based assessments**: These assessments measure the participant's ability to apply the skills and knowledge they learned in the training. They can be administered in various ways, such as through practical exercises, simulations, or case studies.<br>**Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cybersecurity. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews.<br>**Behavioural assessments**: These assessments measure the participants' actual behaviour in relation to cybersecurity. They can be administered in various ways, such as through observation, self-report, or peer-report. |

### 3.1.3 Syllabus of the Training Module 1: Cybersecurity Essentials and Management

Table 4: Cybersecurity essentials and management: Training Module 1 syllabus.

| Main topics | Suggested content |
|---|---|
| **Ethical Conduct and Professionalism** | • Understand ethical principles and guidelines for cybersecurity professionals, including confidentiality, integrity, and availability (CIA).<br>• Recognise and avoid conflicts of interest, safeguard confidential information, and protect privacy rights.<br>• Implement ethical decision-making processes. |
| **Foundational Knowledge of Cybersecurity** | • Define cybersecurity and its importance in today's digital world.<br>• Introductions to basic cybersecurity terminology and concepts.<br>• Explore the CIA triad: Confidentiality, Integrity, and Availability.<br>• Understand the different types of current cybersecurity threats and vulnerabilities (high-level overview).<br>• Recognise the role of the human error in cybersecurity breaches (high-level overview). |
| **Cybersecurity Body of Knowledge (CyBoK)** | • Gain a comprehensive overview of cybersecurity concepts, practices, and methodologies.<br>• Learn about various cybersecurity frameworks and models: overview of ISO/IEC 27001, ECSF, NIST Cybersecurity Framework and CyBoK.<br>• Overview of the Cybersecurity Body of Knowledge. |
| **Threats and vulnerabilities** | • Identify and classify different types of cybersecurity threats, including malware, phishing, and social engineering.<br>• Analyse common vulnerabilities found in software, systems, and networks.<br>• Understand the impact of threats and vulnerabilities on cybersecurity |

| Main topics | Suggested content |
|---|---|
| | posture.<br>• Vulnerability assessments and penetration tests to identify and prioritise vulnerabilities.<br>• Implement vulnerability management strategies to remediate vulnerabilities.<br>• Monitor and respond to cybersecurity incidents effectively |
| **Human Factor Considerations** | • Recognise the importance of human psychology in cybersecurity.<br>• Identify and address human behaviour risks, such as social engineering, password reuse, and phishing scams.<br>• Implement security awareness and training programmes to educate and empower users.<br>• Manage user access and privileges to restrict unauthorised access.<br>• Implement strong password policies and enforce two-factor authentication (2FA). |
| **Secure Architecture Design and Implementation** | • Design secure network architectures and system configurations.<br>• Implement access control mechanisms to restrict unauthorised access.<br>• Employ data encryption techniques to protect sensitive information.<br>• Employ secure coding practices to prevent vulnerabilities in software development.<br>• Implement network segmentation to isolate critical assets.<br>• Implement intrusion detection and prevention systems (IDS/IPS) to monitor and protect networks. |
| **Security Controls Selection and Implementation** | • Evaluate and select appropriate security controls.<br>• Implement security controls effectively to mitigate vulnerabilities.<br>• Monitor and maintain security controls to ensure continuous effectiveness. |
| **Data Security and Privacy by Design** | • Understand data privacy and security including privacy by design and security by design principles.<br>• Implement data security measures to protect confidentiality, integrity, and availability of data.<br>• Design for privacy by incorporating data protection principles into the development lifecycle. |
| **Cybersecurity Governance: Policies, Procedures, Standards, Methodologies and Frameworks** | • Develop and implement cybersecurity policies and procedures.<br>• Establish and manage security standards and guidelines.<br>• Utilise cybersecurity frameworks to achieve organisational goals.<br>• Implement governance mechanisms to ensure accountability and oversight. |
| **Cybersecurity Governance: Cybersecurity Related Laws, Regulations and Legislations including** | • Stay informed about cybersecurity laws, regulations, and legislations.<br>• Implement compliance programmes to ensure adherence to legal and regulatory requirements.<br>• Conduct regular security audits to assess compliance and identify gaps.<br>• Consult legal and ethical experts for guidance on cybersecurity matters. |

| Main topics | Suggested content |
|---|---|
| **Auditing, Legal and Ethical Compliance** | |
| **Information and Cyber Security Risk Management (ISRM)** | • Conduct comprehensive risk assessments to identify and prioritise cybersecurity risks.<br>• Develop and implement risk mitigation strategies to address identified risks.<br>• Monitor and manage cybersecurity risks on an ongoing basis.<br>• Continuously evaluate and update risk management plans. |
| **Soft/Professional Skills** | **Soft Skills and Leadership Development:**<br>• Develop strong communication and interpersonal skills to collaborate effectively.<br>• Demonstrate leadership qualities to motivate and guide cybersecurity teams.<br>• Build relationships with stakeholders to foster trust and support.<br>• Adapt to changing cybersecurity threats and technological advancements. |
| | **Effective Communication and Documentation:**<br>• Communicate cybersecurity risks, policies, and procedures clearly and concisely.<br>• Document cybersecurity incidents and remediation efforts systematically.<br>• Maintain accurate and up-to-date cybersecurity documentation.<br>• Tailor communication for different audiences. |
| | **Self-Reflection and Continuous Learning:**<br>• Continuously self-assess cybersecurity knowledge and skills.<br>• Stay up-to-date with the latest cybersecurity trends and technologies.<br>• Participate in professional development training and certifications.<br>• Embrace a growth mindset and actively seek opportunities to learn. |

### 3.1.4 CyberSecPro General Presentation Template for the Training Module

In order to generalise the presentations of the CSP training modules, trainers should follow a generic format and a common structure comprising several aspects that can be of interest to the participants. Among the aspects, we highlight at least two relevant ones: on the one hand, the features of the training module and its possible interest to the participants, and, on the other hand, the logistics of the training module should be kept in mind by those interested in taking the training module. In other words, the presentations of the training modules should contain at least the following information, organised in two main explanatory blocks:

- **WHO-WHAT-WHY**. It addresses three relevant questions: (i) WHO can attend the training modules, detailing the profiles of the audience, as well as information on the main training providers; (ii) WHAT topics are relevant to acquire the necessary knowledge and comply with the established CSP Knowledge Area(s) to which the module belongs to; and (iii) explain briefly WHY this training module could be relevant for the participants.

- **WHEN-WHERE-HOW**. This second block adds information about the logistics of the CPS training module and the conditions for its realisation: (i) WHEN (semester, spring, autumn, summer) the module is being offered by the CSP partner (ii) WHERE (physical, virtual or hybrid) the module is to be offered and (iii) HOW the module is organised in terms of the content provider, contact information, assessment, among others.

Depending on the training module and its needs, both blocks can be expanded with additional information, allowing providers to intensify the value of their respective modules. In this respect, we recommend following a common rationale based on the following steps when designing the presentation of the modules:

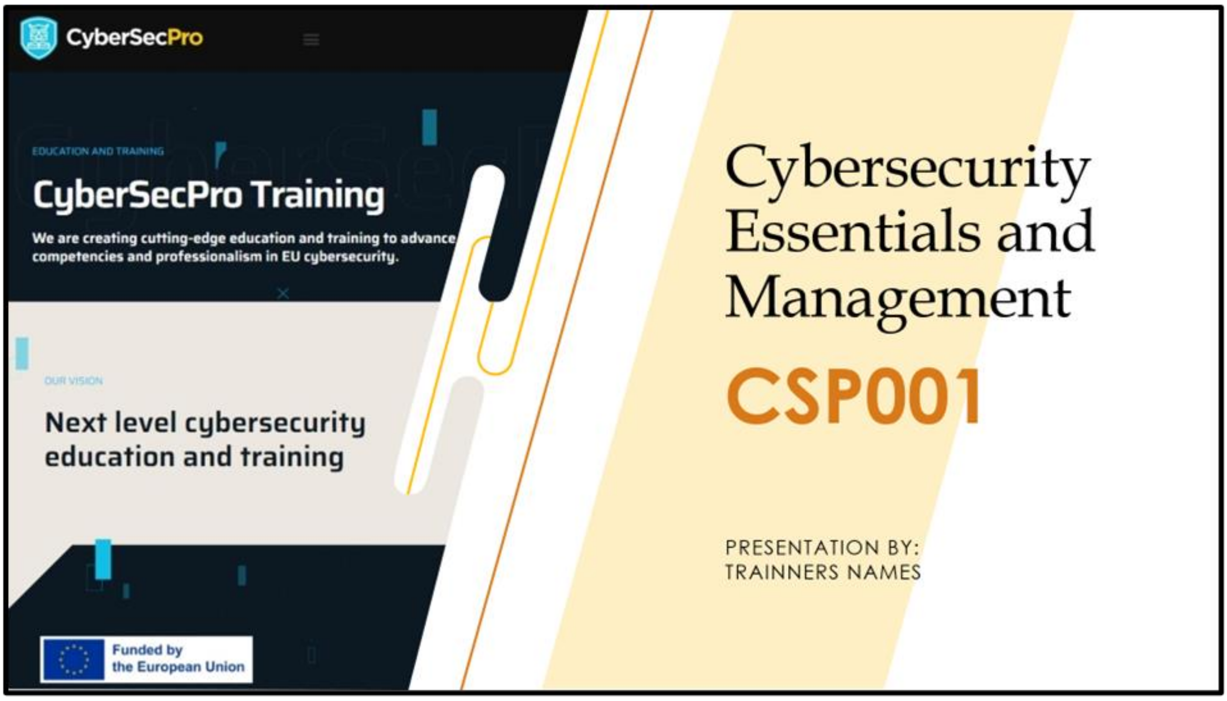
1. **Start the presentation with general information about the training module**, indicating the main title of the training module, its code, the details of the main trainers in charge of presenting the training module, logos and funding entities, but also a clear overview of the presentation of the training module, which should outline the discussion points of the presentation.
2. **An overview of the training module**, considering the two main blocks mentioned above, where it is essential to clarify (and in a very summarised form) "WHO-WHAT-WHY" the module is essential to participants, and "WHEN-WHERE-HOW" with summarised information about the logistic of the training module.
3. **Specific information about the training module contains**:
    a. **Value propositions** establishing the level of the training module, language and all the benefits that can bring the learning process to participants, such as knowledge and skills to be acquired, practical developments, provision of certificates, etc.
    b. **The training module** by expanding the information on the two main blocks mentioned above. This includes the specification of the main topics corresponding to the syllabus and following a simplified structure, approximated schedules, the learning outcomes, the profile of each trainer implied in the module, where and how the module will be taken, knowledge and skills to be developed and how (e.g., per topic), etc.
    c. **Work methodology and practical developments** in order to clarify the learning process and the development of the practical exercises, e.g., through flipped classroom, gamification, project-based exercises, etc.
    d. **Evaluation method** that allows participants to successfully complete the training module and obtain the certificate at the predetermined level.
    e. **Preconditions** that help ensure the continuity of the learning process include background knowledge and associated prerequisites, technical tools that must be installed before the training module or installation conditions, etc.
    f. **Additional material to support the learning process** includes references, videos, links to other CSP Training modules, biographical links, etc. This information should be completely optional.
    g. **General information about the registration process**, explaining how participants could reach the training module and any other practical information to enable proper registration and access.
4. **End of the presentation**, thank the audience for their attendance and include some contact information.

In summary, all this design content and preparation for the overall presentation of the training modules is detailed in Table 5 and its template presented in Figure 2.

Table 5: Generic presentation template summary.

| **Start the presentation with general information about the training module** | |
|---|---|
| 1 slide | Main title of the training module, code and details of the trainers in charge of presenting the training module, logos, funding entities |

| | |
|---|---|
| 1 slide | Overview of the presentation of the training module |
| **An overview of the training module** | |
| 1 slide | WHO-WHAT-WHY |
| 1 slide | WHERE-WHEN-HOW |
| **Specific information of the training module - WHO-WHAT-WHY-WHEN-WHERE-HOW** | |
| 1/+ slides | Value propositions |
| 1/+ slides | The training module |
| 1/+ slides | Work methodology and practical developments |
| 1/+ slides | Evaluation method |
| 1/+ slides | Preconditions |
| 1/+ slides | Additional material to support the learning process |
| 1/+ slides | General information about the registration process |
| **End of the presentation** | |
| 1 slide | Acknowledgements and contact information |



CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

Next level cybersecurity education and training

Cybersecurity Essentials and Management

CSP001

PRESENTATION BY:
TRAINNERS NAMES

Figure 2: CyberSecPro PPT template.

### 3.1.5 CyberSecPro General Video Teaser template for the Training Module

A video teaser consists of an audio-visual resource of short duration (approximately 70 seconds), whose main goal is to (i) present the objectives of the training module and (ii) capture prospective participants' attention. To achieve these goals, the resource should contain straightforward messages that present the main features and contents of the corresponding CSP training module. The video presentation has the start and ending; mainly, it must concord with the two explanatory blocks detailed in the body sections: (i) **WHO-WHAT-WHY**, and (ii) **WHEN-WHERE-HOW**.

To generalise the dialogue associated with the CyberSecPro General Presentation, we propose below (see Table 6) a generic video teaser development approach that could be adapted to the CSP training modules and their respective needs. The template will also facilitate the relevant training providers' design, development, and publication of all CSP training modules.

Table 6: Generic video teaser development template.

| Approach | More specification about the approach | Number of video frames and seconds | Content | Total seconds (maximum recommended) |
|---|---|---|---|---|
| **Start of the video teaser** | Start of the module teaser and presentation | Frame 1 – 10* seconds | **Audio-visual assets**: the CyberSecPro logo must be visible, code of the training module, and the logo of each main training provider + piece of instrumental music.<br>**Text**: name of the project ("CyberSecPro"), and name of the training module | 10* seconds |
| **WHO-WHAT-WHY** | Information of the target audience (for who) | Frame 2 – 10* seconds | **Audio-visual assets**: the CyberSecPro logo must be visible + piece of instrumental music (continuation to the previous frame)<br>**Text with bullets**: "It has been designed for:<br>• Target audience 1,<br>• Target audience 2,<br>• Target audience 3<br>• …."<br>the most representative ones. | 10* seconds |
| | Information related to the content of the training module by remarking or emphasising the main topics of training | Frame 3 – 10* seconds | **Audiovisual assets**: the CyberSecPro logo must be visible + piece of instrumental music (continuation to the previous frame)<br>**Text with bullets**: "This course aims to cover the following main topics:<br>• "TOPIC-1,<br>• TOPIC-2,<br>• TOPIC-3<br>• …." | 10* seconds |

| | | | | | |
|---|---|---|---|---|---|
| | (what is covered) | | the most representative ones. | | |
| | Main learning outcomes and skills achieved after finishing the training (why the training is important) | Frame 4 – 10* seconds | **Audio-visual assets**: the CyberSecPro logo must be visible + piece of instrumental music (continuation to the previous frame)<br>**Text with bullets**: “As a result, the module aims to enhance: | | 10* seconds |
| | | | • Learning outcome 1,<br>• Learning outcome 2,<br>• Learning outcome 3<br>• ….”<br>the most representative ones. | • Soft Skill 1,<br>• Soft Skill 2,<br>• Soft Skill 3<br>• ….”<br>the most representative ones. | |
| | | | • Special mentioned of the gain knowledge and skills are relevant to ECSF professional roles | • List the appropriate ECSF Professional Role(s) that matching with the training learning outcomes | |
| **WHEN-WHERE-HOW** | Brief explanation about when and where the training module will be offered (when-where) | Frame 5 – 10* seconds | **Audio-visual assets**: the CyberSecPro logo must be visible + piece of instrumental music (continuation to the previous frame)<br>**Text with bullets**:<br>• *Season*<br>• *Virtual/physical/hybrid*<br>• *Schedules and frequencies* | | 10* seconds |

| | | | | |
|---|---|---|---|---|
| | A brief detail about the learning method, evaluation and any other practicalities (how) | Frame 6 – 10* seconds | **Audio-visual assets**: the CyberSecPro logo must be visible + piece of instrumental music (continuation to the previous frame)<br>**Text with bullets**:<br>• *Pedagogical methods, together with multiple exercises and practical activities to consolidate a better professional career in the future.*<br>• *Evaluation methods*<br>• *Any other practicalities*<br>• *Certification of Attendance* | 10* seconds |
| **End of video teaser** | The final part of the video should remark on the existence of the DCM platform, and that all information is available on the DCM. | Frame 7 – 5* seconds | **Audio-visual assets**: the CyberSecPro logo must be visible, and a picture related to the DCM platform + piece of instrumental music (continuation to the previous frame)<br>**Text with bullets**: “All the complementary information, including the whole access and registration process, is also available on the DCM platform” | 5* seconds |
| | The end | Frame 8 – 5* seconds (equivalent to the frame 1) | **Audio-visual assets**: the CyberSecPro logo must be visible, code of the training module, and the logo of each main training provider + piece of instrumental music (continuation to the previous frame)<br>**Text**: name of the project (“CyberSecPro”), and name of the training module | 5* seconds |
| | | | | **70* seconds** |

* only indicative time and partners/training providers can adjust the timeline according to their training needs

#### 3.1.5.1 Analysis and recommendation of free and open-source video editors

This section considers free and open-source video editors that may be used to create video teasers. Partners are encouraged to adopt and use tools that yield the same high-quality video for all implemented modules in creating video teasers. Table 7 provides a comparison of different editors and their corresponding vital features. Most of the available open-source video editors have similar functions and editing options. Their main difference lies in the templates they can provide and the level of difficulty in using them. In [31], we can find a comparison of 15 open-source video editors for Windows, Linux and Mac, most of them supporting FFmpeg. The latter corresponds to a free and open-source software project, which compiles libraries and tools for multimedia processing (audio, video, subtitles and related metadata) and is compatible with multiple formats.

Table 7: Essential features of video editors for creating video teasers.

| Video editor | Features | Reference |
|---|---|---|
| **Movavi** | • Free software editor with purchase option<br>• Compatible for Windows and macOS<br>• Illustrative videos with quality images and effects<br>• It requires edition technical knowledge for its use | [32] |
| **Filmora Video Editor** | • Free editor with purchase option<br>• Compatible for Windows and macOS<br>• Illustrative videos with quality images and effects (2D, 3D)<br>• It offers multiple types of templates.<br>• It requires edition technical knowledge for its use | [33] |
| **OpenShot Video Editor** | • Open-source editor compatible for Windows, Linux, macOS and ChromeOS<br>• Illustrative videos with quality images and effect (2D, 3D)<br>• +70 languages<br>• Very documented [4], including tutorial videos.<br>• Support for Advanced AI for motion tracking, object detection, stabilisation.<br>• It requires edition technical knowledge for its use | [34] |
| **ShotCut** | • Open-source editor based on FFmpeg.<br>• Compatible for Windows, Linux, macOS<br>• Illustrative videos but limited editions | [35] |
| **LightWorks** | • Free software editor with purchase option<br>• Compatible for Windows, Linux and macOS<br>• Illustrative videos with quality images and effects<br>• Documented with a lot of tutorial videos in YouTube [8] | [36] |
| **Flowblade** | • Open-source editor compatible with Linux with support for many rendering formats<br>• Limited documentation<br>• It requires edition technical knowledge for its use | [37] |
| **Blender** | • Open-source editor compatible for Windows and macOS<br>• Illustrative videos with high-quality images and the capacity to add 3D animations.<br>• The tool is not user-friendly; by incorporating advanced 3D video creation options.<br>• It requires edition technical knowledge for its use | [38] |
| **KDEnlive** | • Open-source editor compatible for Windows, Linux and macOS<br>• Illustrative videos with high-quality images | [39] |

| Video editor | Features | Reference |
|---|---|---|
| | • It requires edition technical knowledge for its use.<br>• The tool does not apply GPU acceleration, making rendering slow [30], with limited exportations | |
| **DEEPBRAIN AI** | • Realistic AI avatars, natural text-to-speech, and powerful text-to-video capabilities all in one AI video editor.<br>• Accelerate video projects at scale with AI-powered video creation.<br>• Good for creating professional asynchronous training materials | [40] |
| **PICTORY AI** | • Easy Video Creation for Content Marketers<br>• Natural text-to-speech, and powerful text-to-video capabilities all in one AI video editor.<br>• Accelerate video projects at scale with AI-powered video creation.<br>• Good for creating professional asynchronous training materials | [41] |

In [31], it is possible to find a comparative tool considering the compatibility with the different operating systems and their functions for 4K editing and motion tracking. From the solutions analysed, Blender, KDEnlive, and Filmora are the most complete regarding the latter two features and are compatible with Windows and macOS. KDEnlive is also compatible with Linux. The most effective and efficient ones are the AI based tools including Deepbrain and Pictory. Partners may, therefore, consider these tools in their video teaser creation.

### 3.1.6 CyberSecPro Training Module Evaluation Template-Trainees and Trainers

Annex C provides documents that have been finalised templates based on the combined development work of WP2, WP3, and D4.1. This template is intended to be used by trainees and trainers to provide feedback on the CyberSecPro training modules. The feedback is essential for continuously improving the CSP training programme and ensuring that it meets the needs of participants and HEIs in the future. These templates will be developed on a DCM system, and feedback could be collected online, too.

### 3.1.7 Transparency Guidelines- CyberSecPro Education and Training Material

This section outlines the guidelines for creating and using CyberSecPro education and training materials. These guidelines ensure adherence to the standards set forth in the CyberSecPro Grant Agreement No. 101083594, specifically regarding Intellectual Property Rights (IPR), Referencing Practices, and Professional and Ethical Conduct.

Compliance with Grant Agreement: Particular attention should be paid to Section 2: Rules for Carrying Out the Action and Section 3: Grant Administration of the CyberSecPro Grant Agreement.

State-of-the-Art Considerations: The consortium partners have established additional guidelines for material creators and users due to the innovative nature of the project, which includes the use of AI in education and training. It requires a guideline for the CyberSecPro Professional Training material creators and users.

High-Level Guidelines for CyberSecPro Materials: Following are the high-level guidelines, and all the partners uses when CyberSecPro Education and Training Material posted on publicly.

1. **Creative Commons License:**
   a. All CyberSecPro education and training materials are licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0): https://creativecommons.org/
   b. This license allows for non-commercial sharing, adaptation, and remixing of the materials, but requires attribution to the EU CyberSecPro project (https://www.cybersecpro-project.eu/) and mention of the license used.
   c. Derivative works must also be shared under the same CC BY-NC-SA 4.0.
2. **Academic References:**

All materials must include appropriate academic references formatted according to the grant agreement policy.

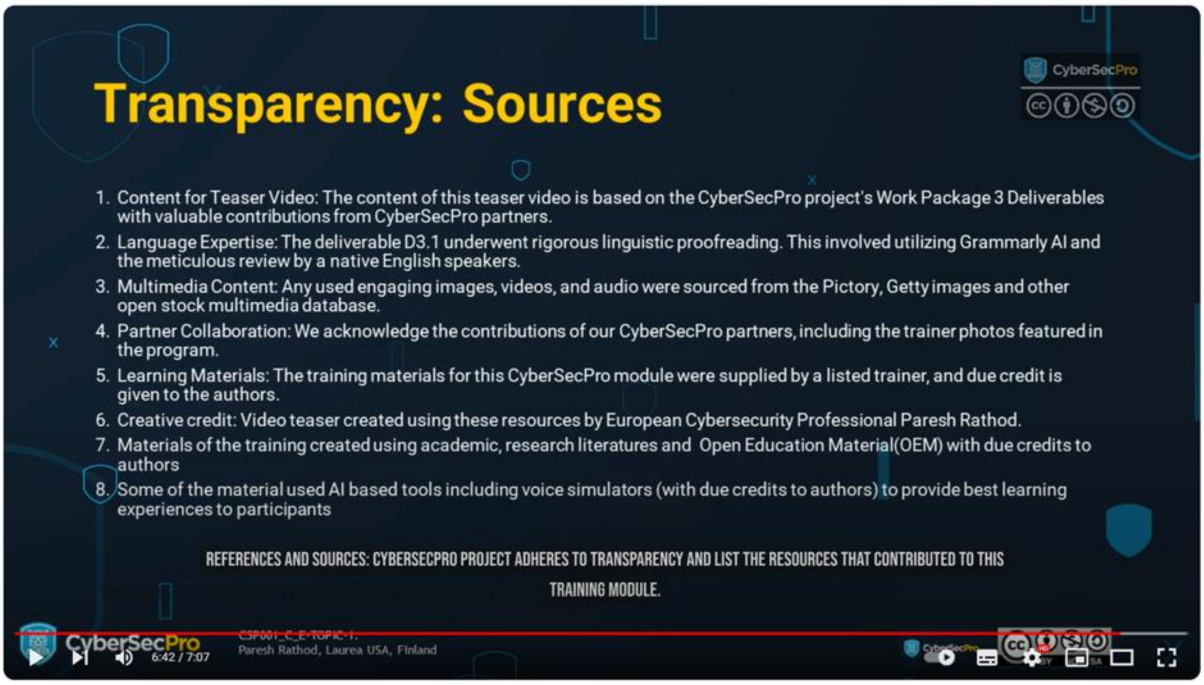
3. **Transparency and Source Declaration:**

All sources used in the materials must be declared in accordance with fairness and transparency policies. This includes:

   a. *Multimedia sources*: A general declaration should be included, such as: "Multimedia Content: Engaging images, videos, and audio were sourced from the Google database. Some materials may have utilized AI-based tools to enhance the learning experience. All sources are properly credited within the materials."
   b. *AI Tools*: In addition to academic references, a general declaration is required for using AI tools.

4. **Avoiding Complexity:**
   a. Recognizing that the CyberSecPro project is an EU initiative for public benefit, the partners have agreed to minimize complexities that might restrict fair use of the materials. The CC BY-NC-SA 4.0 license already provides a strong foundation for fair use.
   b. Therefore, a high-level and simple transparency declaration, along with proper academic references, is sufficient. No need to trivialise the matter that restricts usage as public good to users.

Figure 3 provides additional guidance to display the CC license logo, simple transparency declaration of sources (in addition to another slide on Academic Reference).



Transparency: Sources

1. Content for Teaser Video: The content of this teaser video is based on the CyberSecPro project's Work Package 3 Deliverables with valuable contributions from CyberSecPro partners.
2. Language Expertise: The deliverable D3.1 underwent rigorous linguistic proofreading. This involved utilizing Grammarly AI and the meticulous review by a native English speakers.
3. Multimedia Content: Any used engaging images, videos, and audio were sourced from the Pictory, Getty images and other open stock multimedia database.
4. Partner Collaboration: We acknowledge the contributions of our CyberSecPro partners, including the trainer photos featured in the program.
5. Learning Materials: The training materials for this CyberSecPro module were supplied by a listed trainer, and due credit is given to the authors.
6. Creative credit: Video teaser created using these resources by European Cybersecurity Professional Paresh Rathod.
7. Materials of the training created using academic, research literatures and Open Education Material(OEM) with due credits to authors
8. Some of the material used AI based tools including voice simulators (with due credits to authors) to provide best learning experiences to participants

REFERENCES AND SOURCES: CYBERSECPRO PROJECT ADHERES TO TRANSPARENCY AND LIST THE RESOURCES THAT CONTRIBUTED TO THIS TRAINING MODULE.

Figure 3. Example to display the CC license logo (video teaser of the the CyberSecPro training module 1 for energy sector).

## 3.2 Module 2 - Human Factors and Cybersecurity

### 3.2.1 Target Audience and Goals

This training module comprehensively explores human factors in cybersecurity, targeting IT professionals, security experts, and business leaders. In alignment with pedagogical requirements, the curriculum spans individual and organisational levels, addressing strategic, operational, and tactical aspects. It covers diverse topics and delves into the psychological, social, and organisational factors influencing security behaviours. The module instils a commitment to integrity, guiding participants with ethical principles for responsible knowledge use due to some subject matters, thus emphasising academic honesty and professional ethics.

**Goals:**

Beyond technical expertise, it cultivates an understanding of human aspects of cybersecurity, including social engineering techniques used by malicious actors, social and organisational aspects to give learners an understanding of the responsibility essential for navigating the intricate cybersecurity landscape.

### 3.2.2 Description of Training Module 2: Human Factors and Cybersecurity

Table 8: Human factors and cybersecurity: Training Module 2 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.* | **CSP002** |

| | | |
|---|---|---|
| | *The Generic Model Syllabi as a simple code, as seen in the next column.* | |
| **Content** | **Module title**<br>*The Title of the training module* | **Human Factors and Cybersecurity** |
| | **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Human Aspects of Cybersecurity<br>• Human Elements in Cybersecurity<br>• The Human Dimension in Cybersecurity<br>• Navigating Cyber Threats: The Human Element<br>• Elements of Cyberpsychology<br>• Humans in Cybersecurity<br>• Human Centric Cyber Defence |
| | **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module overview**<br>*High-level module overview* | This training module provides participants with the necessary knowledge and skills about human aspects of cybersecurity at the individual and organisational levels as well as at the strategic, operational, and tactical levels. |
| | **Module description**<br>*Indicates the main purpose and description of the 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. |
| | **Knowledge Area(s)** | Mainly KA2 and some overlapping topics with KA7 |

| | | |
|---|---|---|
| | *Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | |
| | **Category(s) of capabilities**<br>*Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | Refer and check D4.1. |
| | **Learning outcomes and targets**<br>*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, participants will have gained the following:<br>**Knowledge:**<br>• Understanding of the human element's role in cybersecurity.<br>• Knowledge of common human errors and vulnerabilities exploited in cyberattacks.<br>• Awareness of psychological and social factors influencing security decisions.<br>• Understanding of organisational culture's impact on cybersecurity posture.<br>• Knowledge of effective communication strategies for cybersecurity collaboration.<br>• Insights into decision-making at different levels in cybersecurity.<br>• Awareness of best practices for designing and implementing cybersecurity training programmes.<br>• Understanding of emerging trends and challenges in cybersecurity related to human factors.<br>**Skills:** |

| | | |
|---|---|---|
| | | • Identifying and analysing human factors contributing to cybersecurity risks.<br>• Assessing and mitigating risks associated with human vulnerabilities.<br>• Developing and implementing effective communication strategies for security awareness and collaboration.<br>• Making informed security decisions considering human factors and data.<br>• Designing and evaluating cybersecurity training programmes for different audiences.<br>• Staying up to date on emerging trends and best practices in human factors and cybersecurity.<br>**Competencies:**<br>• Critical thinking about the human element in cybersecurity.<br>• Problem-solving to address human-related security risks.<br>• Effective communication with diverse stakeholders about cybersecurity.<br>• Collaboration across domains to build a robust security culture.<br>• Decision-making based on data, analysis, and understanding of human factors.<br>• Adaptability to evolving threats and challenges in the cybersecurity landscape. |
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Ethical and Professional Practices<br>• Introduction to Human Aspects of Cybersecurity<br>• Psychological and Social Factors in Cybersecurity<br>• Human Vulnerabilities in Cybersecurity<br>• Organisational Culture, Communication, and Cybersecurity<br>• Communication and Collaboration Across Domains<br>• Decision Making at Strategic, Operational, and Tactical Levels |

| | | |
|---|---|---|
| | | • Training, Awareness, and Communication Programmes<br>• Future Trends, Challenges, and the Role of Communication |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Management/ Logistics** | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Basic IT training (or) EU Digital Competence (DigComp) Framework level know-how. |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | Mainly ECSF Profile: Cybersecurity Educator.<br>Minor content matches with others ECSF profile including:<br>• Chief Information Security Officer (CISO)<br>• Cybersecurity Researcher<br>• Cybersecurity Risk Manager |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |

| | | |
|---|---|---|
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | *Check online in CyberSecPro DCM System for current information on the specific module instantiation. Some of the aspects considered are listed below:*<br>**Knowledge-based assessments**: These assessments measure the participant's knowledge of the material that was covered in the training. They can be administered in various ways, such as through multiple-choice questions, essay questions, or fill-in-the-blank questions.<br>**Performance-based assessments**: These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. They can be administered in a variety of ways, such as through practical exercises, simulations, or case studies.<br>**Attitudinal assessments**: These assessments measure the participants' attitudes and beliefs about cybersecurity. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews.<br>**Behavioural assessments**: These assessments measure the participant's actual behaviour |

| | | |
|---|---|---|
| | | about cybersecurity. They can be administered in a variety of ways, such as through observation, self-report, or peer-report. |

### 3.2.3 Syllabus of the Training Module 2: Human Factors and Cybersecurity

Table 9: Human factors and cybersecurity: Training Module 2 syllabus.

| Main topics | Suggested content |
|---|---|
| **Introduction to Human Aspects of Cybersecurity** | • Definition and significance: An overview of the human element's role and importance in the cybersecurity landscape.<br>• Interplay between technology and human behaviour: Exploring how human actions interact with and influence technological systems.<br>• Cybersecurity landscape: A brief look at the current state of cybersecurity threats and defences.<br>• Common misconceptions: Debunking myths related to the human aspect of cybersecurity.<br>• Cost of neglecting the human element: Understanding the consequences of overlooking human factors in security.<br>• Setting the stage: Examining real-world incidents to highlight the consequences of human errors. |
| **Psychological and Social Factors in Cybersecurity** | • Understanding cognitive biases: Understanding inherent biases that influence security decisions.<br>• Social engineering techniques: Exploring social engineering approaches used to deceive individuals.<br>• Psychology behind phishing: Understanding the psychological triggers exploited in phishing attacks.<br>• Role of trust: Examining how trust dynamics impact security behaviours.<br>• Group dynamics: Investigating how group interactions can influence individual security actions.<br>• Emotional factors: Understanding how emotions like fear and curiosity affect cybersecurity decisions. |
| **Human Vulnerabilities in Cybersecurity** | • Cataloguing common errors: Listing frequent human mistakes that lead to security breaches.<br>• Insider threats: Differentiating between intentional malicious actions and unintentional human errors within an organisation.<br>• Impact of stress and fatigue: Understanding how physical and mental strain can compromise security decisions.<br>• Challenge of maintaining vigilance: Discuss the difficulty of staying consistently alert to security threats.<br>• Case studies: Analysing real incidents to understand the role of human vulnerabilities.<br>• Mitigation strategies: Identifying solutions to reduce risks |

| Main topics | Suggested content |
|---|---|
| | associated with human vulnerabilities. |
| **Organisational Culture, Communication, and Cybersecurity** | • Organisational values: Exploring how a company's core values influence its security posture.<br>• Ripple effect: Understanding how a single decision can have widespread implications for an organisation's security.<br>• Leadership's role: Understanding how different leadership styles influence setting communication standards and security priorities.<br>• Feedback loops: Discussing the significance of continuous feedback in improving cybersecurity measures.<br>• Proactive security culture: Strategies to cultivate an anticipatory approach to threats.<br>• Overcoming resistance: Addressing challenges in changing established culture and security practices. |
| **Communication and Collaboration Across Domains** | • Effective communication: Understanding factors of successful communication in cybersecurity.<br>• Challenges in collaboration: Identifying obstacles in inter-domain cooperation and their solutions.<br>• Building bridges: Strategies to enhance collaboration across domains.<br>• Role of mediators: Understanding the importance of intermediaries in facilitating effective communication.<br>• Case studies: Analysing instances of successful and failed collaborations.<br>• Communication tools: Having an oversight of platforms and tools that aid in effective communication. |
| **Decision Making at Strategic, Operational, and Tactical Levels** | • Layers of decision-making: Understanding the different levels of decision-making in cybersecurity.<br>• Interdependence of decisions: Understanding how decisions at one level can influence actions at other levels.<br>• Communication channels: Discuss appropriate communication methods for each decision-making level.<br>• Balancing speed and accuracy: Strategies to make timely yet informed decisions.<br>• Role of data: Emphasising the importance of data-driven decision-making.<br>• Case studies: Analysing real-world decisions made during cybersecurity incidents. |
| **Training, Awareness, and Communication Programmes** | • Impactful training: Designing effective targeted cybersecurity training programmes that meet participant needs.<br>• Continuous education: The importance of continued professional development in adapting to evolving threats.<br>• Tailored training: Customising training programmes for targeted groups.<br>• Feedback: The significance of integrating feedback to improve training modules. |

| Main topics | Suggested content |
|---|---|
| | • Measuring effectiveness: Techniques to assess the success and impact of training initiatives.<br>• Leveraging technology: Using modern technological tools to enhance training experiences. |
| **Future Trends, Challenges, and the Role of Communication** | • Anticipating threats: Predicting upcoming cybersecurity challenges.<br>• Emerging technologies: Understanding how new technological trends will shape human interactions and communication patterns.<br>• Interdisciplinary collaboration: Understanding and leveraging the growing need for cooperation across various fields in cybersecurity.<br>• Remote workforces: Preparing for security challenges posed by decentralised teams and workforces.<br>• AI and automation: Exploring the influence of artificial intelligence on human behaviour in cybersecurity.<br>• Staying ahead: Strategies to remain updated in a rapidly evolving cybersecurity environment. |

## 3.3 Module 3 - Cybersecurity Risk Management and Governance

### 3.3.1 Target Audience and Goals

This module is designed for IT professionals, security professionals, and business leaders who need to understand the subject.

- IT Professionals: Security analysts, network administrators, system engineers, incident responders, and IT security managers.
- Business Professionals: CEOs, CFOs, board members, risk management professionals, and compliance officers.
- Non-Technical Staff: Employees with access to sensitive data and systems, such as HR personnel, finance staff, and sales representatives.

**Goals:**

- Develop a comprehensive understanding of cybersecurity risks: Participants will learn to identify, assess, and prioritize cyber threats to their organisation's assets.
- Implement effective risk management strategies: The training will equip participants with the knowledge and tools to develop, implement, and maintain effective cybersecurity risk management frameworks.
- Enhance governance practices: Participants will gain insights into establishing clear roles, responsibilities, and accountability for cybersecurity within the organisation.
- Improve compliance with regulations: The training will cover relevant cybersecurity regulations and standards, helping participants understand how to achieve compliance.
- Foster a culture of cybersecurity awareness: The program will equip participants with the skills to communicate cybersecurity risks effectively and promote a culture of security awareness within the organisation.

- Build decision-making capabilities: Participants will learn how to make informed decisions about cybersecurity investments and resource allocation based on risk assessments.
- Increase overall cybersecurity posture: By achieving these goals, the training ultimately aims to improve the organisation's overall cybersecurity posture and resilience against cyberattacks.

### 3.3.2 Description of Training Module 3: Cybersecurity Risk Management and Governance

Table 10: Cybersecurity risk management and governance: Training Module 3 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | **CSP003** |
| **Content** | **Module title**<br>*The Title of the training module* | **Cybersecurity Risk Management and Governance** |
| | **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Information Security Risk Management<br>• Security Management<br>• Trust Management<br>• Risk Assessment and Management<br>• Enterprise Risk Management<br>• Risk Assessment and Mitigation<br>• Risk Control and Governance<br>• Risk Minimization Strategies<br>• Risk Analysis and Remediation<br>• Risk Mitigation and Compliance<br>• Strategic Risk Planning<br>• Risk Avoidance and Management<br>• Threat Management and Mitigation<br>• Risk Intelligence and Decision-Making |
| | **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |

| | |
|---|---|
| **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Module overview**<br>*High-level module overview* | This course focuses on acquainting participants with the principles and requirements for Information Systems (IS) security and privacy. The main phases of an Information Security Management System (ISMS) implementation are described as defined within ISO/IEC 27001. Risk Management and Risk Assessment methodologies are introduced based on standards and best practices. Security Management will involve the development of security reports (e.g. Risk Treatment Plan, Security Policy, Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), and Security Procedures) |
| **Module description**<br>*Indicates the main purpose and description of the module.* | This module introduces the basic principles, standards, legislation, policies, rationale and requirements of an Information Security Management System based on the ISO/IEC 27000x standards. Since risk management is part of the requirements of an ISMS, this module also aims to provide the basic principles, phases and methodologies for implementing it. Mitigation Actions (technical and non-technical) and procedures will be introduced, assessed and evaluated, as well as development of security reports. |
| **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | Mainly with KA3 and some minor topics from KA1, KA4 |
| **Category(s) of capabilities** | Refer and check D4.1. |

| | | |
|---|---|---|
| | *Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | |
| | **Learning outcomes and targets**<br>*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, participants will have gained the following:<br>**Knowledge:**<br>• Basic definitions related to Information Security Management Systems and Information Security Governance<br>• Risk Management: Basic phases and principles for an effective risk management methodology.<br>• Standards and Methodologies of Risk Management<br>• Legal and Policies related to Risk Management<br>• Measurements, Scales and Metrics of Risks<br>• Technical and non-Technical Mitigation Actions<br>**Skills:**<br>• Applying a suitable methodology for Information Security Risk Management and Risk Assessment.<br>• Analysing Information Security Risk utilising different methodologies.<br>• Creating policies, procedures and processes compliant with the requirements of the current version of the ISO/IEC 27000x series of standards.<br>• Selecting and implementing appropriate mitigation actions and controls.<br>• Developing security policies and procedures<br>• Developing Business Continuity Plans and Disaster Recovery Plans.<br>• Implementing cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards. |

| | | |
|---|---|---|
| | | • Analysing and consolidating the organisation’s quality and risk management practices.<br>• Enabling business asset owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks.<br>• Enabling employees to understand, embrace and follow the controls.<br>• Building a cybersecurity risk-aware environment.<br>• Communicating, presenting and reporting to relevant stakeholders.<br>• Proposing and managing risk-sharing options<br>**Competencies:**<br>• Lead and participate in strategic, operational, and tactical cybersecurity discussions.<br>• Lead the design, development, operation and improvement of an Information Security Management System.<br>• Support the organisation in the audits of an Information Security Management Systems.<br>• Advanced knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices<br>• Knowledge of cyber threats, threats taxonomies and vulnerabilities repositories<br>• Knowledge of risk-sharing options and best practices<br>• Knowledge of technical and organisational controls that appropriately mitigate cybersecurity risks.<br>• Knowledge of cybersecurity-related technologies and controls<br>• Knowledge of monitoring, implementing, testing and evaluating the effectiveness of the controls |

| | | |
|---|---|---|
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Introduction to information security and cyber security, including CIA triad.<br>• Risk Management Approaches<br>• Risk Concepts and Models<br>• Risk management-related standards.<br>• The scope and purpose of an Information Security Management System<br>• Information Security Risk Management definitions and principles<br>• ISO/IEC 27005 and ISO 31000 basic structure<br>• Risk Management Process and Context establishment.<br>• Threats and vulnerabilities<br>• Risk Evaluation, Risk Treatment and Risk Acceptance<br>• Measurements and Metrics<br>• Risk assessment and management processes and methodologies.<br>• Cybersecurity Maturity Models Requirements / Auditing practices<br>• Security Reports |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Management/ Logistics** | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module |

| | | |
|---|---|---|
| | | instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Basic IT training (or) EU Digital Competence (DigComp) Framework level know-how |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | • Chief Information Security Officer (CISO)<br>• Cyber Legal, Policy & Compliance Officer<br>• Cybersecurity Auditor<br>• Cybersecurity Risk Manager |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes** | *Check online in CyberSecPro DCM System for current information on the specific module* |

| | | |
|---|---|---|
| | *Assessment elements and high-level process to determine participants have achieved the learning outcomes* | *instantiation. Some of the aspects considered are listed below:*<br>**Knowledge-based assessments**: These assessments measure the participant's knowledge of the material that was covered in the training. The instructor can administer them orally during the course/seminar delivery.<br>**Performance-based assessments**: These assessments measure the participant's ability to apply the skills and knowledge that they learned in the training. These assessments are delivered during the course as part of the "practical" exercises.<br>**Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cybersecurity. The instructor notices the behaviour of the participant and extracts conclusions regarding the understanding. |

### 3.3.3 Syllabus of Training Module 3: Cybersecurity Risk Management and Governance

Table 11: Cybersecurity risk management and governance: Training Module 3 syllabus.

| Main topics | Suggested content |
|---|---|
| **Introduction to Information Security and Cybersecurity** | • This topic covers the basic terms and definitions the participants should be acquainted with to facilitate better / uniform understanding.<br>• The terms introduced in this section are derived from various standards (e.g., ISO/IEC), initiatives (e.g., NIST, ENISA) and guidelines, standards, legal and EU policies related to security management will be presented and analysed.<br>• Cybersecurity Risk Management Foundation, Risk Management Lifecycle and Governance |
| **The ISO/IEC 27k family of standards** | • Various standards are explored as part of this topic; in particular, the ISO/IEC 27k family of standards is explored.<br>• This overview includes ISO/IEC 27000 - which provides vocabulary and basic principles, standards containing requirements (e.g., ISO/IEC 27001:2022, ISO 27799:2016, ISO/IEC 27006), standards providing guidance and best practices on controls (e.g., ISO/IEC 27002:2022, ISO/IEC 27035-1 and others)) |
| **The scope and purpose of an ISMS** | • Within this topic, information is provided on what an ISMS is and the benefits and objectives of its implementation.<br>• Within this topic, the differences between implementing individual controls and implementing an ISMS are demonstrated. |
| **The PDCA** | • This topic describes the Plan-Do-Check-Act cycle and the relationship between the phases and the Information Security Management System. The |

| Main topics | Suggested content |
|---|---|
| | advantages and alternatives of this approach are also discussed. |
| **The requirements of ISO/IEC 27001 - clauses 4-10** | • This topic discusses in depth the requirements of the clauses of ISO/IEC 27001. Through a series of examples and exercises, participants are guided through the implementation steps and mandatory requirements of an Information Security Management system.<br>• The topics discussed include context, information security policy, roles and responsibilities, audits, change management, objectives, management review, monitoring and measurement and corrective actions.<br>• This topic presents and discusses the mandatory minimum documentation related to an ISO/IEC 27001:2022 implementation. |
| **Information Security Risk Management definitions and principles**<br>**Threats and vulnerabilities**<br>**ISO/IEC 27005 and ISO 31000 basic structure** | • This topic introduces the key component of an Information Security Management System - risk management.<br>• Specifically, the basic terms related to risk management are introduced as well as the phases proposed by international standards (i.e., ISO 31000 and ISO/IEC 27005) as needed for an effective implementation of information security risk management.<br>• The phases of a risk management process are explained, and an exercise is performed to cover the following phases:<br>• Context - Risk identification - Risk Analysis - Risk Evaluation - Risk Treatment.<br>• The phases of recording, reporting, monitoring, review, and communication are described. |
| **Threat Models and Technical Vulnerabilities and Measurements** | • Technical and non-technical threats and vulnerabilities will be analysed. The various metrics systems (e.g. CVE, CVSS4, CWE ) will be presented and illustrated with various examples. |
| **Other Risk Assessment methodologies and tools** | • This topic introduces a list of risk assessment methodologies and tools.<br>• Exercises are carried out using a specific methodology and a tool. Comparisons are made between the approaches and results. The ENISA interoperability framework is described and discussed. |
| **The Annex A of ISO/IEC 27001:2022** | • This topic describes the concept behind Annex A covering controls and risk management. The structure of the controls (in themes) and the usage of attributes are described.<br>• Examples of controls (one per theme) will be incorporated in an implementation exercise considering the guidance of ISO/IEC 27002. Non-technical mitigation actions will be presented. |
| **Security Policies and Procedures** | • The development of security policy, BCP, DRP and procedures based on standards will be covered in this section. The human element in the risk assessment process will be analysed. |
| **Certificates and certification** | • This topic introduces the concept of certification, conformity assessment-related standards and methodologies. |

| Main topics | Suggested content |
|---|---|
| **Cybersecurity Maturity Models and Open Issues** | • Cybersecurity maturity models have been introduced in the last ten years. Some of them have already been incorporated into laws or are being presented as best practices for organisations.<br>• This topic presents the history and rationale of the maturity models in cybersecurity. Specific examples of cybersecurity maturity models are presented, and their usage is explained through relevant exercises. Cybersecurity challenges in managing the risks of the emerging technologies will be analysed. |

## 3.4 Module 4 - Network Security

### 3.4.1 Target Audience and Goals

Considering the list of stakeholders defined in section 2.1, this CSP training module is designed for a broad audience and is especially relevant for individuals who are:

- IT professionals, system administrators, network engineers and service providers who are responsible for managing and securing communication networks and their integrated systems.
- Security professionals protect organisations from cyber-attacks from networks, such as the Internet, wireless networks, mobile networks, and virtualised networks.
- Business leaders who need to understand the risks and costs of cyber-attacks from external/internal networks.
- Training professionals, instructors or educators to build and improve their syllabi and/or cybersecurity skills for teaching.
- Cybersecurity enthusiasts with an interest in learning and improving practical skills in the topic of network security.
- Recent graduates who need to delve into specific topics and improve skills to embark on their professional careers with an emphasis on topics related to network security, related problems, and defence tools.

**Goals:**

Thus, the main objective of this module is to explore the security of different types of networks, not only looking at the evolution of traditional network architectures but also on the security of advanced networks such as the Internet of Things (IoT), mobile networks, or Software-Defined Networks (SDN). In addition, this module also aims to lay the security foundations to identify the security vulnerabilities and risks that may seriously affect the proper functioning of an interconnected environment, as well as to understand how to protect the corresponding communication systems using current protection tools, hardening and good practices.

### 3.4.2 Description of Training Module 4: Network Security

This module is designed for IT professionals, security professionals, and business leaders who need to understand the weaknesses of network systems and the most relevant security mechanisms that help to create robust deployments against potential network threats.

Table 12: Network security: Training Module 4 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | **CSP004** |
| **Content** | **Module title**<br>*The Title of the training module* | **Network Security** |
| | **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Threats and Network Hardening<br>• Basic Principles of Network Security<br>• Network Security Management<br>• Secure Design and Management of Communication Systems<br>• Cyber Network Defence<br>• Network Protection Strategies<br>• Secure Networking Practices<br>• Information Security Networking<br>• Cyber Defence for Networks<br>• Network Threat Prevention<br>• Securing Network Infrastructure<br>• Digital Network Defence<br>• Data Network Security<br>• Network Risk Management<br>• System and Network Security |
| | **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |

| | | |
|---|---|---|
| | **Module overview**<br>*High-level module overview* | This module will provide participants with the necessary knowledge to identify and address the possible security problems and threats associated with the emergence of various types of communication networks and their implicit protocols. In this training process, participants will also learn how these protocols can be used to the benefit of attackers and what can be done to prevent their exploits. The module will also provide ways of post-attack policies in case of a successful attack and measures to ensure privacy and anonymity in communication systems. |
| | **Module description**<br>*Indicates the main purpose and description of the module.* | This module's main objective is to provide a clear vision of the different types of communication systems, network structures, components and protocols involved. This knowledge will be key not only to lay the necessary foundations on how attacks exploit network traffic and the components that makeup communication networks but also to know how to identify potential and/or common threats in order to prevent them.<br>Thus, this module covers a wide range of topics with practical usefulness in multiple today's application scenarios and ecosystems such as IoT and their variants. This feature also obliges us to offer content not only with a theoretical approach but also with a mainly practical approach, where trainees will gain experience and skills by addressing a set of exercises and practical activities. |
| | **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | Mainly KA5 |

| | | |
|---|---|---|
| | **Category(s) of capabilities**<br>*Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | Refer and check D4.1. |
| | **Learning outcomes and targets**<br>*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, participants will have gained the following:<br>**Knowledge:**<br>• General knowledge of communication infrastructures and models as well as the emergence of modern networks and technologies.<br>• Knowledge of the most common vulnerabilities and threats in specific network systems (in traditional networks, mobile networks, virtualised systems, or distributed systems) and their associated protocols.<br>• Knowledge of the most relevant security protocols, such as SSL/TLS and IPSec, and their importance for the protection of systems and communication networks.<br>• Knowledge of the most relevant security mechanisms, such as firewalls and IDS/IPS, to protect network perimeters and access to private domains, such as corporate networks.<br>• Knowledge of the most relevant security mechanisms to protect the endpoints of communication, such as a client and a server, but also the interconnection elements between a client and a server.<br>• Knowledge of the most relevant security mechanisms to protect those advanced communication infrastructures such as mobile networks or virtualized systems.<br>• Knowledge of privacy and anonymity in network management, ensuring the protection of end nodes and their location.<br>• Knowledge of the most relevant authorization models (including access control models, roles and permissions, access monitoring) and authentication methods (including biometrics, dongles, single-sign-on)<br>• Understanding the fundamental concepts of network security and using cryptographic techniques to ensure secure |

| | | |
|---|---|---|
| | | transmissions among interconnected nodes in computer networks.<br>• Knowledge of building secure network architecture by considering network segmentation and isolation. Additionally, understanding the usability of critical security devices such as Firewalls, IDS/IPS, VPNs, tunnelling, and others.<br>• Understanding the basic security mechanisms, services, and attacks in the OSI reference model.<br>**Skills:**<br>• Planning and designing secure networks according to the most general recommendations and following good security practices.<br>• Analysing communication scenarios and identifying possible misconfigurations or vulnerabilities that could lead to security risks or threats.<br>• Configuring systems following basic security principles (e.g., user control, port control, etc.).<br>• Identifying and applying those security elements or mechanisms that contribute to improving the security of a communication system.<br>**Competencies:**<br>• Know how to identify possible misconfigurations or errors that may lead to significant security risks.<br>• Lead the design, configuration and deployment of communication systems.<br>• Support the organisation in hardening its systems and enhancing secure communications.<br>• Knowledge of existing security technologies, mechanisms and protocols, useful to protect any peer-to-peer communication.<br>• Knowledge of recommendations and best practices for securing end nodes and interconnection elements. |

| | | |
|---|---|---|
| | | • Knowledge of privacy weaknesses and existing mechanisms to address threats |
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Basic network fundamentals, architectures, and protocols<br>• Common weaknesses, attacks and threat models in communication networks<br>• Main security protocols embedded in the traditional communication stack.<br>• Policy models, composition and automation<br>• Perimeter defence and protection tools<br>• Security of end communication nodes and of interconnection systems<br>• Security in advanced network infrastructures<br>• Security of general- and special-purpose systems<br>• Privacy and anonymity in communication networks<br>• Authorisation models and authentication methods<br>• Security mechanisms, services, and attacks in OSI reference model<br>• Secure Network Architecture and Design<br>• Cryptographic Techniques for Ensuring Secure Data Transmission |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Management/ Logistics** | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as* | Check online in CyberSecPro DCM System for current information on the specific module |

| | | |
|---|---|---|
| | *periodicity (e.g., even after the end of the CSP programme).* | instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Basic knowledge of cybersecurity essentials (Module 1), and optionally, experience with operating systems, network setup and protocols |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | • Cyber threat Intelligence Specialist<br>• Cybersecurity Architect<br>• Cybersecurity Auditor<br>• Cybersecurity Researcher<br>• Penetration Tester |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)** | Check online in CyberSecPro DCM System for current information on the specific module |

| | | |
|---|---|---|
| | *Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | *Check online in CyberSecPro DCM System for current information on the specific module instantiation. Some of the aspects considered are listed below:*<br>Knowledge-based assessments: As mentioned above, this type of assessment allows trainers to measure the level of knowledge received during the training phase. The assessment can be carried out in a variety of ways, such as through multiple-choice questions or tests, essay questions, or fill-in-the-blank questions.<br>In fact, frequent tests may be planned in which participants could, for example, search the web, open their textbooks, and look things up easily. Tests are not to make participants fail and stress them but to make them remember and recall knowledge and skills. That is why they should be frequent and with all sources available, where trainers may also give hints during tests if some of the participants do not understand the test questions or the purpose of the question.<br>**Performance-based assessments**: Depending on the theoretical contents, assessment may require measuring the level of participants' ability to apply practical skills, the degree of research and knowledge learned. Therefore, these evaluations can be managed in a variety of ways, such as through practical exercises, simulations, or case studies.<br>**Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cybersecurity and their active implication during the training phase. Thus, this evaluation can be carried out in a variety of ways, such as through observation, self-report, peer-report, use of resources (e.g., forums) and regular access to the DCM platform. |

### 3.4.3 Syllabus of Training Module 4: Network Security

Table 13: Network security: Training Module 4 syllabus.

| Main topics | Suggested content |
|---|---|
| **Basic network fundamentals, architectures and protocols** | • Emergence of Networks: Evolution from the internet to advanced network ecosystems<br>• Network Infrastructure and Protocols: Understanding |

| Main topics | Suggested content |
|---|---|
| | internet architecture and fundamental protocols (TCP/IP, IP addressing, routing)<br>• Network Architectures: Common architectures (client-server, peer-to-peer, cloud)<br>• Interconnection Devices: Firewalls, switches, routers, their roles and vulnerabilities<br>• Introduction to Network Security: Basic security concepts, threats, and challenges |
| **Common weaknesses, attacks and threat models in communication networks** | • Common Weaknesses and Bad Practices: Misconfigurations, weak passwords, outdated software<br>• Threat Models and Common Attacks: Denial-of-service, malware, social engineering, data breaches<br>• Early Detection: Abnormal system behaviour, log analysis, anomaly detection, intrusion detection systems<br>• Offensive Tools and Techniques: Understanding how attackers exploit vulnerabilities.<br>• Demonstration of attacks, replication, testing, mitigation, and post-attack remedies |
| **Main security protocols embedded in the traditional communication stack** | • Application-Layer Security: HTTPS, TLS, secure coding practices<br>• Transport-Layer Security: TCP/IP security features, VPNs.<br>• Network-Layer Security: Firewalls, access control lists.<br>• Link-Layer Security: Port-based authentication, encryption standards.<br>• Perimeter Defence Techniques: Network segmentation, intrusion detection/prevention systems |
| **Perimeter defence and protection tools** | • Network segmentation.<br>• Virtual private networks<br>• Intrusion detection and prevention<br>• Deception and feedback<br>• Network security monitoring |
| **Policy models, composition and automation** | • Access control mechanisms and segregation of duties<br>• Strategies to improve information system security.<br>• Benefits and limitations for identifying patterns, detecting anomalies, and enhancing proactive security measures.<br>• Threat detection, risk assessment, and decision-making in information systems |
| **Security of end communication nodes and of interconnection systems** | • Protecting Endpoints: Antivirus, endpoint detection and response systems<br>• Hardening Operating Systems: Securing Windows and Linux systems<br>• Securing Interconnection Devices: Firewalls, switches, routers |

| Main topics | Suggested content |
|---|---|
| **Security in advanced network infrastructures** | • Introduction to distributed and advanced networks<br>• Distributed and Decentralised Networks: Blockchain, mesh networks, and security considerations<br>• Mobile Network Security: Threats and defences for mobile communication<br>• Virtualised Network Security: Security challenges and solutions in virtual environments |
| **Security of general- and special-purpose systems** | • Ensuring robust security measures within a system<br>• Unique security challenges arising from special purposes systems.<br>• Risk mitigation and protection against potential vulnerabilities in special purpose systems |
| **Privacy and anonymity in communication networks** | • Introduction to anonymous communications: Different levels of anonymity and their purpose<br>• Anonymity Strategies: Tor, VPNs, encryption techniques<br>• Location Tracking and Mitigation: Understanding tracking methods and countermeasures.<br>• Privacy Considerations: Balancing security and privacy needs |
| **Authorisation models and authentication methods** | • Comprehensive management of authorization mechanisms in various systems<br>• Distinction between authentication and authorisation<br>• Access control models (DAC, MAC, RBAC), role definitions and permissions, access monitoring for security breaches<br>• Establishing the identity and validity of entities engaging in human-to-system or system-to-system interactions<br>• Overview on authentication methods (e.g., passwords, biometrics, dongles, single sign-on, etc.) |
| **Secure Network Architecture and Design** | • Building a secure network design and architecture<br>• Network segmentation and isolation approaches.<br>• Security zones and conduits to meet particular security requirements for industrial assets.<br>• Security devices for protecting interconnected terminals within computer networks (firewalls, IPS/IDS, tunnelling, VPNs, etc.) |
| **Cryptographic Techniques for Ensuring Secure Data Transmission** | • Basics of cryptography, including encryption and decryption<br>• Differences between symmetric and asymmetric encryption approaches<br>• Digital signatures for ensuring the authentication of data transmission |

| Main topics | Suggested content |
|---|---|
| **Security mechanisms, services, and attacks in OSI reference model** | • Details about the OSI security architecture and X.800 security architecture for OSI<br>• Different security services offered by each protocol layer.<br>• Security mechanisms for achieving security objectives |

## 3.5 Module 5 - Data Protection and Privacy Technologies

### 3.5.1 Target Audience and Goals

This module is designed for IT professionals, security professionals, and business leaders who need to understand the subject.

**Target Audience:**

- IT professionals: Data security analysts, privacy engineers, cloud architects, system administrators.
- Business professionals: Compliance officers, data governance specialists, HR personnel, marketing managers.
- Non-technical staff: Any employee handling personal data, regardless of their technical expertise.

**Goals:**

- Raise awareness of data protection and privacy regulations: Equip participants with a clear understanding of key data protection regulations (GDPR, CCPA, etc.) and their implications for their organisation.
- Understand privacy-enhancing technologies (PETs): Introduce and explain the purpose and application of various PETs like anonymization, pseudonymisation, and differential privacy.
- Build data protection compliance knowledge: Provide the tools and knowledge to implement effective data protection measures, including data mapping, risk assessments, and data breach response plans.
- Develop best practices for data handling: Instruct participants on responsible data collection, storage, access control, and disposal practices.
- Empower individuals to protect their data: Equip participants with the knowledge and skills to manage their own personal data privacy settings and choices.
- Foster a culture of data privacy: Encourage participants to advocate for and champion data privacy within their organisations.

### 3.5.2 Description of Training Module 5: Data Protection and Privacy Technologies

This module is designed to develop a comprehensive understanding and learn practices of the data protection and privacy technologies. The training module aims to empower both individuals and organisations to navigate the evolving landscape of data protection and privacy with confidence and compliance.

Table 14: Data protection and privacy technologies: Training Module 5 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|

| | | |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | **CSP005** |
| **Content** | **Module title**<br>*The Title of the training module* | **Data Protection and Privacy Technologies** |
| | **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Privacy Technologies<br>• Privacy by Design<br>• Data Security and Protection<br>• Data Privacy<br>• Privacy and Online Rights |
| | **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module overview**<br>*High-level module overview* | This module will provide policies and practices for data protection in terms of security flaws and disastrous events. Further, this comprehensive training module equips individuals and organisations with the knowledge and skills to navigate the ever-evolving landscape of data protection and privacy. |
| | **Module description**<br>*Indicates the main purpose and description of the module.* | The module provides practical training and participants will gain a deep understanding of key regulations, privacy-enhancing technologies (PETs), and best practices for implementing effective data protection programmes. Master key encryption methods, anonymity techniques, zero-knowledge infrastructure setup, data security policies, and incident response strategies. Manage social engineering and phishing attacks, implement organised scarcity for effective security, anonymise data sharing, create digital authorities, and even learn how to revive systems after disasters. Gain the |

| | | |
|---|---|---|
| | | knowledge and skills to navigate the complex world of data protection with confidence. |
| | **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | Mainly KA6. |
| | **Category(s) of capabilities**<br>*Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | Refer and check D4.1. |
| | **Learning outcomes and targets**<br>*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, participants will have gained the following:<br>**Knowledge:**<br>• Regulations and Standards: Understand key data privacy regulations (e.g., GDPR and others) and their implications for organisations and individuals.<br>• Privacy-Enhancing Technologies (PETs): Identify and explain the purpose, benefits, and limitations of various PETs (e.g., anonymization, encryption, differential privacy).<br>• Data Protection Best Practices: Gain knowledge of effective data security measures, data retention and deletion practices, and data breach response plans.<br>• Emerging Trends: Recognise the impact of new technologies (e.g., AI, big data) on data privacy and ethical considerations.<br>**Skills:** |

| | | |
|---|---|---|
| | | • Data Mapping and Inventory: Identify and map data flows within an organisation.<br>• Data Protection Impact Assessments (DPIAs): Conduct risk assessments for data processing activities and implement mitigation strategies.<br>• Security Policy and Procedure Development: Define and implement data security policies and procedures, including access control and MFA.<br>• Data Anonymisation and Sharing Techniques: Apply PETs to anonymize data and enable secure data sharing.<br>• Incident Response: Develop and implement a plan for responding to data breaches and security incidents.<br>**Competencies:**<br>• Critical Thinking: Analyse complex data privacy scenarios and recommend appropriate solutions.<br>• Problem-solving: Identify and address data protection challenges within organisations.<br>• Communication and Collaboration: Effectively communicate data privacy risks and best practices to stakeholders.<br>• Adaptability: Stay informed about evolving data privacy regulations and technologies, and adapt practices accordingly.<br>• Ethical Decision-Making: Balance the need for data security with individual privacy rights and ethical considerations. |
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Introduction to Data Protection and Privacy<br>• EU Data Protection Landscape<br>• Data Protection Lifecycle Management<br>• Privacy-Enhancing Technologies (PETs)<br>• Implementing Effective Data Protection Programmes and Compliance<br>• Building a Culture of Privacy |

| | | |
|---|---|---|
| | | - The Future of Data Protection and Privacy |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Management/ Logistics** | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Basic IT training (or) EU Digital Competence (DigComp) Framework level know-how |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | - Cyber Legal, Policy & Compliance Officer<br>- Cybersecurity Architect<br>- Cybersecurity Auditor<br>- Cybersecurity Implementer |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |

| | | |
|---|---|---|
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | Several questionnaires examine how well students have comprehended basic ideas regarding the architecture that should be used according to the scenario and the infrastructure. Further, refer and check online CyberSecPro DCM System for current information. |

### 3.5.3 Syllabus of Training Module 5: Data Protection and Privacy Technologies

Table 15: Data protection and privacy technologies: Training Module 5 syllabus.

| Main topics | Suggested content |
|---|---|
| **Introduction to Data Protection and Privacy** | • Key data protection regulations (international): GDPR, CCPA, HIPAA, and other relevant laws<br>• Data privacy principles: Fairness, transparency, accountability, and data subject rights<br>• Importance of data protection and privacy: Legal, ethical, and reputational risks<br>• Evolving privacy landscape: Emerging technologies and their impact on privacy |
| **EU Data Protection Landscape** | • Introduction to key regulations: GDPR, ePrivacy, EU initiatives and national variations.<br>• Key data protection principles: Transparency, accountability, purpose limitation, data minimization.<br>• Data subjects' rights: Access, rectification, erasure, portability, objection.<br>• Cross-border data transfers: International considerations and |

| Main topics | Suggested content |
|---|---|
| | limitations. |
| **Data Protection Lifecycle Management** | • Data mapping and inventory: Identifying and classifying personal data.<br>• Privacy impact assessments (PIA): Evaluating data processing risks.<br>• Data security and technical safeguards: Encryption, access controls, incident response.<br>• Data breach notification and reporting requirements. |
| **Privacy-Enhancing Technologies (PETs)** | • Introduction to PETs and their role in data protection.<br>• Anonymisation and pseudonymisation techniques.<br>• Differential privacy and secure multi-party computation.<br>• Homomorphic encryption and other emerging PETs. |
| **Implementing Effective Data Protection Programmes and Compliance** | • Developing and implementing a data protection program.<br>• Data governance and accountability frameworks.<br>• Building a culture of privacy within your organisation.<br>• Compliance audits and best practices. |
| **Building a Culture of Privacy** | • Privacy by design and by default: Integrating privacy into development processes.<br>• Employee privacy awareness training: Empowering employees to protect data.<br>• Communication and transparency: Building trust with data subjects.<br>• Governance and accountability: Defining roles and responsibilities for data protection.<br>• Case Studies: Analysing real-world examples of successful privacy programmes. |
| **The Future of Data Protection and Privacy** | • Emerging trends and challenges: Artificial intelligence, big data, and the future of data privacy<br>• Ethical considerations and best practices: Balancing innovation with data protection<br>• Staying ahead of the curve: Continuous learning and adapting to change<br>• Opportunities for innovation: Leveraging privacy-enhancing technologies for competitive advantage |

## 3.6 Module 6 - Cyber Threat Intelligence

### 3.6.1 Target Audience and Goals

This training module provides a comprehensive knowledge, skills and competences of cyber threat intelligence (CTI) principles, methodologies, and tools. This module is designed for IT professionals, security professionals, and business leaders who need to understand the subject.

**Target Audience:**

- Security professionals (analysts, incident responders, SOC operators)
- IT professionals (network administrators, system engineers).
- Risk management professionals.
- Compliance officers.

**Goals:**

- Develop a foundational understanding of CTI concepts and principles.
- Gain hands-on experience with CTI tools and techniques.
- Learn to integrate CTI into existing security processes.
- Enhance threat detection, prevention, and response capabilities.
- Improve decision-making based on real-time threat intelligence.

### 3.6.2 Description of Training Module 6: Cyber Threat Intelligence

This module is designed for IT professionals, security professionals, and business leaders who need to understand the current threat landscape context, including threat intelligence properties and sharing. This training module provides a comprehensive understanding of cyber threat intelligence (CTI) principles, methodologies, and tools. Participants will learn to collect, analyse, and disseminate threat information to proactively identify, assess, and mitigate cyber threats.

Table 16: Cyber threat intelligence: Training Module 6 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | **CSP006** |
| **Content** | **Module title**<br>*The Title of the training module* | **Cyber Threat Intelligence** |
| | **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Cybersecurity Intelligence Collaboration<br>• Threat Intelligence Exchange<br>• Security Threat Information Sharing<br>• Cyber Threat Analysis and Collaboration<br>• Intelligence-driven Cyber Defence<br>• Threat Information Collaboration<br>• Cybersecurity Intelligence Fusion<br>• Collaborative Threat Mitigation |

| | | |
|---|---|---|
| | | • Intelligence-led Cybersecurity<br>• Threat Sharing and Analysis<br>• Cybersecurity and Threat Hunting<br>• Threat Modelling Approaches |
| | **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module overview**<br>*High-level module overview* | The module aims to provide learners with an overview of threat intelligence and management. It allows the learners to analyse the known and unknown threats and determine a course of action to tackle them. |
| | **Module description**<br>*Indicates the main purpose and description of the module.* | The module explains the underlying properties and principles associated with cyber threats within an organisational setting. This module focuses on the current landscape of threats with the emerging trends in threat hunting and intelligence. Upon completing the module, the learners can adopt the knowledge and skill to analyse the threats in their organisational context. |
| | **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | Mainly with KA7 and some minor topics from KA1, KA8 |

| | | |
|---|---|---|
| | **Category(s) of capabilities**<br>*Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | Refer and check D4.1. |
| | **Learning outcomes and targets**<br>*A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module.* | Upon successful completion of this module, the learner will be expected to be able to demonstrate the:<br>**Knowledge:**<br>• Demonstrate knowledge and understanding of threats to an information and network system.<br>• Taxonomy of cyber threats, actors, and motivations.<br>• Threat intelligence lifecycle and its components.<br>• Variety of threat intelligence sources and their strengths/weaknesses.<br>• Security controls and standards relevant to specific threats.<br>• Vulnerability assessment techniques and tools.<br>• MITRE ATT&CK framework and its application in threat modelling.<br>• Advanced analytical techniques for threat detection and analysis.<br>• Methods for developing and maintaining threat actor profiles.<br>• Effective communication and dissemination of threat intelligence.<br>• Ethical and legal considerations surrounding CTI acquisition and use.<br>• Knowledge on available data sources and collections, how to validate them and how to use the data.<br>• Knowledge on basic and advanced concepts for anomaly detection and log file analysis<br>• Understand how to identify potential threat actors and analyse their tactics.<br>• Knowledge of different threat modelling approaches and an understanding of |

| | | |
|---|---|---|
| | | potential cyber threats and vulnerabilities that could lead to cyber-attacks.<br>**Skills:**<br>• Analyse and interpret various sources of threat intelligence.<br>• Conduct threat modelling and identify vulnerabilities in systems.<br>• Apply advanced analytical techniques to identify and prioritise threats.<br>• Develop and maintain threat profiles for specific adversaries.<br>• Disseminate actionable threat intelligence to different audiences.<br>• Evaluate and select CTI tools and platforms based on specific needs.<br>• Implement and manage a CTI program within an organization.<br>• Align security controls and standards with identified threat profiles.<br>• Communicate threat intelligence effectively in written and verbal formats.<br>• Conduct ethical threat research and responsibly disclose vulnerabilities.<br>**Competencies:**<br>• Critical thinking and problem-solving in the context of cyber threats.<br>• Ability to analyse complex data and identify patterns and trends.<br>• Effectively collaborate and share information with diverse stakeholders.<br>• Adapt to evolving threat landscapes and technologies.<br>• Make informed decisions based on threat intelligence.<br>• Maintain ethical and responsible practices in CTI activities.<br>• Demonstrate effective leadership and communication skills in managing a CTI program. |

| | | |
|---|---|---|
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Foundations of Cyber Threat Intelligence (CTI)-Taxonomy, Lifecycle, Security Controls and Standards<br>• Threat Modelling and Analysis<br>• Data sources and collection<br>• Data analysis and data processing<br>• Threat actors and tactics<br>• Vulnerabilities Assessment Techniques<br>• Advanced Analytical Techniques and Threat Actor Profiling<br>• Threat Intelligence Information Sharing, Dissemination, Communication, and Implementation<br>• Legal and Ethical Considerations<br>• Anomaly detection<br>• Log file analysis.<br>• Practical Threat Modelling and Security Investigation |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Management/ Logistics** | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the* | Check online in CyberSecPro DCM System for current information on the specific module |

| | | |
|---|---|---|
| | *location. If virtual, provide the URL link of the website.* | instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Basic IT and Security Knowledge |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | Mainly, Cyber Incident Responder<br>Additionally,<br>• Cybersecurity Risk Manager<br>• Cyber Threat Intelligence Specialist<br>• Cybersecurity Implementer |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | *Check online in CyberSecPro DCM System for current information on the specific module instantiation. Some of the aspects considered are listed below:*<br>**Formative assessment**: Learner needs to develop a logbook based on the individual exercise covered at the end of each session to |

| | | |
|---|---|---|
| | | demonstrate their understanding of the knowledge covered by the module.<br>**Summative assessment**: Learner needs to produce a 2000-word report at the end of the module by performing a list of tasks to demonstrate the result of threat and vulnerability assessment and control to tackle the threats based on a real-world scenario. |

### 3.6.3 Syllabus of Training Module 6: Cyber Threat Intelligence

Table 17: Cyber threat intelligence: Training Module 6 syllabus.

| Main topics | Suggested content |
|---|---|
| **Foundations of Cyber Threat Intelligence (CTI)** | • Cyber Threats Taxonomy: Classification of threats, threat actors, and motivations.<br>• Threat Intelligence Lifecycle: Collection, analysis, dissemination, and feedback loop.<br>• Sources of Threat Intelligence: OSINT, commercial feeds, malware analysis, vulnerability databases.<br>• Security Controls and Standards: Aligned with identified threats.<br>• Goals of security control, security control types, security control functions, Access control properties, patch management, CIS Critical Security Controls |
| **Data sources and collection** | • Overview on different types of data sources such as public feeds, dark web, malware analysis, security blogs and social media.<br>• Validation and verification of data as well as processes for preparing and processing the collected information.<br>• Automation techniques and tools to optimize data source collection and scalability. |
| **Data analysis and processing** | • Data processing techniques and advanced analytics techniques (data mining and machine learning).<br>• Visualisation and Big Data tools. |
| **Threat actors and tactics** | • Known threat actors, their motives, tactics, techniques and procedures (TTPs).<br>• Identify and classify threat actors.<br>• Analyse the different tactics, techniques and procedures.<br>• Examine their impact on industries and organizations. |
| **Threat Modelling and Analysis** | • Identifying and Prioritizing Assets: Understanding critical infrastructure and data.<br>• Attack Vectors and Threat Actors: Exploiting vulnerabilities and analysing adversary capabilities.<br>• MITRE ATT&CK Framework: Common Attack Techniques, Tactics, and Procedures (TTPs).<br>• Threat Hunting: Proactively searching for malicious activity |

| Main topics | Suggested content |
|---|---|
| | within networks. |
| **Vulnerabilities Assessment Techniques** | • Basic of vulnerability, vulnerability groups, vulnerability exploitation, Zero Day Exploit<br>• Vulnerability types<br>• Identifying and prioritising system vulnerabilities<br>• Vulnerability database and entries<br>• Common vulnerability scoring system- 3.1 and 4.0.<br>• Vulnerability exploitation |
| **Advanced Analytical Techniques and Threat Actor Profiling** | • Indicator of Compromise (IOC) Analysis: Identifying and correlating indicators of attack.<br>• Data Mining and Visualisation: Analysing large datasets for threat patterns.<br>• Machine Learning for CTI: Automating threat detection and classification.<br>• Threat Scoring and Prioritisation: Assessing the severity and immediacy of threats.<br>• Developing Threat Actor Profiles: Understanding motivations, capabilities, and TTPs of specific adversaries. |
| **Cybersecurity Threat Intelligence Information Sharing, Dissemination, Communication, and Implementation** | • Tailoring Intelligence to Different Audiences: Delivering actionable insights to decision-makers.<br>• Threat Reports and Briefings: Communicating threat intelligence effectively.<br>• Collaboration and Information Sharing: Sharing intelligence within and across organizations.<br>• Developing and Implementing a CTI Program: Defining goals, roles, processes, and metrics.<br>• Security Controls and Standards Implementation: Mitigating risks based on identified threats |
| **Anomaly detection** | • Basic concepts of anomaly detection<br>• Understanding how to identify and deal with anomalies in different data sources.<br>• Understanding of statistical models for anomaly detection<br>• Overview on concepts such as normal distribution, multivariate analysis, time series analysis and Bayesian networks.<br>• Real-time anomaly detection in large data streams<br>• Concepts for online learning, stream mining algorithms and hybrid models for continuous monitoring of data streams<br>• Introduction to tools and techniques to detect, classify, and respond to anomalies in real time |
| **Log file analysis** | • Basic concepts and techniques for collecting, processing, and analysing log data from various sources.<br>• Tools and methods to analyse log data, detect patterns and anomalies, identify threats, and investigate security incidents.<br>• Effective use of log analysis as part of security operations and |

| Main topics | Suggested content |
|---|---|
| | to improve the security of systems and networks |
| **Practical Threat Modelling and Security Investigation** | • Overview of threat modelling approaches to identify security vulnerabilities in a system design.<br>• Utilising ThreatGet to investigate potential cyber threats and security vulnerabilities.<br>• Automated estimation of risk , assessment of risk level<br>• Automated suggestion of security mechanisms for risk mitigation |

## 3.7 Module 7 - Cybersecurity in Emerging Technologies

### 3.7.1 Target Audience and Goals

The training module is designed to equip participants with the knowledge and skills necessary to address the unique challenges posed by integrating cutting-edge technologies in various industries. As businesses embrace innovations such as the Internet of Things (IoT), artificial intelligence (AI), blockchain, and 5G, robust cybersecurity measures become paramount. This module aims to provide a comprehensive understanding of the cybersecurity landscape within the context of emerging technologies.

This module is designed for IT professionals, cybersecurity experts, system administrators, and anyone securing systems leveraging emerging technologies.

**Target Audience:**

- IT professionals (security analysts, system engineers, cloud architects).
- Developers and engineers working with emerging technologies.
- Business professionals seeking to understand the security implications of new technologies.
- Compliance officers and risk management professionals.

**Goals:**

- Raise awareness of cybersecurity risks associated with emerging technologies.
- Understand the security characteristics and vulnerabilities of different emerging technologies.
- Learn best practices for securing applications, data, and infrastructure in emerging technology environments.
- Develop skills for identifying, assessing, and mitigating cybersecurity threats in emerging technologies.
- Gain practical experience with relevant security tools and techniques.

### 3.7.2 Description of Training Module 7: Cybersecurity in Emerging Technologies

Table 18: Cybersecurity in emerging technologies: Training Module 7 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)* | **CSP007** |

| | | |
|---|---|---|
| | *The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | |
| **Content** | **Module title**<br>*The Title of the training module* | **Cybersecurity in Emerging Technologies** |
| | **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Security Challenges in Emerging Technologies<br>• Protecting Emerging Tech: Cybersecurity Considerations<br>• Securing Future Technologies: Cyber Threats and Solutions<br>• Cyber Risks in Emerging Tech Landscapes<br>• Safeguarding Innovation: Cybersecurity in New Technologies<br>• Emerging Tech Security: Addressing Cyber Threats<br>• Cyber Defence for Emerging Technological Landscapes<br>• Ensuring Security in Cutting-Edge Technologies<br>• The Intersection of Cybersecurity and Emerging Tech<br>• Future Tech Security: Navigating Cyber Challenges |
| | **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module overview**<br>*High-level module overview* | The training module is designed to equip participants with the knowledge and skills necessary to address the unique challenges posed by integrating cutting-edge technologies in various industries. As businesses embrace innovations such as the Internet of Things (IoT), artificial intelligence (AI), blockchain, and 5G, robust cybersecurity measures become |

| | |
|---|---|
| | paramount. This module aims to provide a comprehensive understanding of the cybersecurity landscape within the context of emerging technologies. |
| **Module description**<br>*Indicates the main purpose and description of the module.* | This training module explores the unique cybersecurity challenges and best practices associated with emerging technologies, equipping participants with the knowledge and skills needed to protect their environments. Through interactive lectures, hands-on labs, and discussions, participants will gain insights into securing various technologies like the Internet of Things (IoT), cloud computing, blockchain, artificial intelligence (AI), and more. This advanced training delves deep into the intricacies of cybersecurity within the context of emerging technologies. Building upon foundational cybersecurity knowledge, it equips students with specialized skills and strategies for addressing the evolving security landscape brought forth by innovative technologies |
| **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | Mainly KA8 |
| **Category(s) of capabilities**<br>*Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | Refer and check D4.1. |
| **Learning outcomes and targets**<br>*A list of knowledge, skills and competences achieved by the participants as a result of taking a CSP module.* | Upon completing the course, trainees should be well-equipped to address the cybersecurity challenges posed by integrating AI, Cloud, and IoT technologies. They should possess a strong foundation of knowledge, practical skills, and ethical considerations necessary for securing |

| | | |
|---|---|---|
| | | interconnected systems in modern IT environments.<br>Trainees are able to demonstrate following specific learning target including:<br>**Knowledge:**<br>• In-depth understanding of various emerging technologies (IoT, cloud, blockchain, AI, etc.) and their inherent security risks.<br>• Comprehensive knowledge of specific vulnerabilities and attack vectors associated with each technology.<br>• Solid grasp of established security principles and best practices applicable to emerging technology environments.<br>• Awareness of relevant regulations and compliance requirements for securing emerging technologies.<br>• Knowledge of specialized security tools and methodologies for different emerging technology platforms.<br>• Understanding of evolving threats and trends in the emerging technology security landscape.<br>**Skills:**<br>• Critically analyse and evaluate the security implications of specific emerging technologies.<br>• Identify and understand unique vulnerabilities and attack vectors in different technology contexts.<br>• Apply established security principles and best practices to design and implement security solutions for emerging technologies.<br>• Develop and customize security strategies for various use cases across diverse emerging technologies.<br>• Utilise specialized security tools and techniques for securing specific platforms and applications.<br>• Effectively communicate and collaborate with stakeholders on emerging |

|  |  |  |
|---|---|---|
|  |  | technology security challenges and solutions.<br>• Stay informed about new threats and trends, adapting security strategies and practices accordingly.<br>**Competencies:**<br>• Critical thinking and problem-solving in complex emerging technology security scenarios.<br>• Ability to analyse and interpret technical information and develop data-driven security solutions.<br>• Effectively collaborate and communicate technical security concepts to diverse audiences.<br>• Adaptability and agility in responding to the ever-changing emerging technology security landscape.<br>• Strong decision-making skills based on comprehensive understanding of risks and best practices.<br>• Ethical mindset in applying security principles and protecting data privacy in emerging technologies.<br>• Leadership potential in guiding organizations towards secure adoption of emerging technologies |
|  | **Main topics and contents list**<br>*A list of main topics and key content* | • Introduction to Cybersecurity in Emerging Technologies including IoT, cloud, blockchain, AI.<br>• Anomaly Detection Techniques<br>• Securing the Internet of Things (IoT)<br>• Cloud Security<br>• Blockchain Security<br>• Artificial Intelligence (AI) Security<br>• Advanced Topics in Emerging Technology Security including Quantum computing & 5G.<br>• Data Analysis for Cybersecurity<br>• Security Tools and Techniques for Emerging Technologies |

| | | |
|---|---|---|
| | | - The Future of Emerging Technology Security |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Management/ Logistics** | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | - Cyber Threat Intelligence Specialist<br>- Cybersecurity Researcher<br>- Digital Forensics Investigator |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module |

| | | |
|---|---|---|
| | | instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | *Check online in CyberSecPro DCM System for current information on the specific module instantiation. Some of the aspects considered are listed below:*<br>• Use quizzes, class discussions, and short assignments throughout the course to gauge participants' understanding of foundational concepts.<br>• Assign practical projects that require participants to implement security measures in simulated environments, integrating AI, cloud, and IoT technologies. |

### 3.7.3 Syllabus of Training Module 7: Cybersecurity in Emerging Technologies

Table 19: Cybersecurity in emerging technologies: Training Module 7 syllabus.

| Main topics | Suggested content |
|---|---|
| **Introduction to Cybersecurity in Emerging Technologies** | • Overview of emerging technologies and their impact on cybersecurity landscape.<br>• Unique security challenges associated with different technology categories (IoT, cloud, blockchain, AI).<br>• Regulatory and compliance considerations for emerging technologies. |

| Main topics | Suggested content |
|---|---|
| **Anomaly Detection Techniques** | • Introduction to Anomaly Detection: In this section, we will delve into the concept of anomalies, examining their nature as unexpected deviations from the norm. We'll explore anomaly detection's significance and diverse applications, emphasising different types such as point anomalies, contextual anomalies, and collective anomalies. Throughout the session, we'll also address the challenges inherent in anomaly detection, fostering a comprehensive understanding of this critical aspect of cybersecurity.<br>• Machine Learning-Based Method: In this section, we focus on machine learning-based methods and explore various anomaly detection approaches based on supervised and unsupervised machine learning algorithms. We will discuss the evaluation metrics crucial for assessing the effectiveness of these methods, including precision, recall, and F1-score. Through this content, participants will gain insights into the practical applications and considerations of deploying machine learning models for anomaly detection.<br>• Time Series Anomaly Detection: This section will explore the complexities of detecting anomalies in time series data. We will investigate fundamental techniques such as moving averages, exponential smoothing, and the Seasonal-Trend decomposition using Loess (STL) method. Moreover, we'll introduce advanced approaches, including Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN)-based methods tailored for analysing time series data.<br>• Anomaly Detection in Real-World Applications: We will present real use-case scenarios using data from various sources such as IoT devices, network traffic logs, etc. |
| **Securing the Internet of Things (IoT)** | • IoT architecture and its vulnerabilities.<br>• Securing devices, networks, and data in IoT environments.<br>• Best practices for managing IoT security risks. |
| **Cloud Security** | • Cloud security models and shared responsibility model.<br>• Securing cloud infrastructure, applications, and data.<br>• Cloud-specific threats and mitigation strategies. |
| **Blockchain Security** | • Understanding blockchain technology and its security properties.<br>• Vulnerabilities and attack vectors specific to blockchain platforms.<br>• Securing smart contracts and blockchain applications. |
| **Artificial Intelligence (AI) Security** | • Security risks associated with AI, including bias, data privacy, and adversarial attacks.<br>• Methods for securing AI models and training data.<br>• Ethical considerations for AI security practices. |
| **Advanced Topics in Emerging Technology Security** | • Quantum computing and its implications for cryptography.<br>• Securing 5G networks and other emerging communication technologies.<br>• Emerging privacy concerns and data protection considerations. |

| Main topics | Suggested content |
|---|---|
| **Data analysis for cybersecurity** | • In today's rapidly evolving threat landscape, organisations rely on data-driven insights to effectively detect and respond to cyber threats. This module is designed to enable student gain and knowledge and skills in the following areas:<br>• Data analysis techniques and tools for cybersecurity<br>• Application of data analytics and machine learning to specific cybersecurity scenarios to effectively detect and respond to cyber threats |
| **Security Tools and Techniques for Emerging Technologies** | • Specialised security tools and frameworks for different emerging technologies.<br>• Hands-on practice with tools for vulnerability scanning, threat detection, and security configuration. |
| **The Future of Emerging Technology Security** | • Anticipating emerging threats and trends in the security landscape.<br>• Continuous learning and adaptation to keep pace with rapid technological advancements.<br>• Developing a proactive approach to securing emerging technologies. |

## 3.8 Module 8 - Critical Infrastructure Security

### 3.8.1 Target Audience and Goals

Considering the list of stakeholders defined in section 2.1, this CSP training module is designed for a broad audience and is especially relevant for individuals who are:

- IT and OT professionals, IT administrators, engineers and operators, and essential service providers. They are responsible for managing and securing operational network and their integrated information systems.
- Security professionals who protect organisations from specialised cyber-attacks (e.g., Advanced Persistent Threats (APTs) or supply chain attacks).
- CISO and business leaders who need to understand the risks and costs of specialised cyber-attacks from external/internal networks, and particularly against specific domains and critical applications.
- Training professionals, instructors, or educators to build and improve their syllabi and/or cybersecurity skills for teaching.
- Cybersecurity researchers who are interested in finding new research lines.
- Cybersecurity enthusiasts with an interest in learning and improving practical skills in the topic of Critical Infrastructure Security and Resilience.
- Recent graduates who need to delve into specific topics and improve skills to embark on their professional careers with an emphasis on topics related to Critical Infrastructure Security and Resilience.

**Goals:**

The main goal of this module is to explore the security and resilience of specific application environments, considered critical in nature and offering essential services to society and its economy. Therefore, multiple technical, organisational, social, procedural, and legal aspects are covered, while maintaining the perspective of cybersecurity and resilience of critical infrastructures and their operational systems. Other goals include:

- Foster awareness of the criticality of infrastructure and the potential impact of security breaches.
- Understand the unique security challenges and vulnerabilities of different critical infrastructure sectors.
- Develop knowledge of relevant national and international security standards and frameworks.
- Learn risk assessment and mitigation strategies for protecting critical infrastructure assets.
- Build skills for incident response, recovery, and crisis management in critical infrastructure environments.
- Enhance communication and collaboration among stakeholders for effective critical infrastructure security.

### 3.8.2 Description of Training Module 8: Critical Infrastructure Security

This module is designed for IT professionals, security professionals, and business leaders who need to understand and practice the critical infrastructure security.

Table 20: Critical infrastructure security: Training Module 8 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | **CSP008** |
| **Content** | **Module title**<br>*The Title of the training module* | **Critical Infrastructure Security** |
| | **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Protecting Vital Infrastructure: Security Measures<br>• Critical Systems Security: Safeguarding Infrastructure<br>• Securing Essential Services and Infrastructure<br>• Critical Infrastructure Protection: Security Strategies<br>• Infrastructure Resilience and Security<br>• Safeguarding Critical Assets: Infrastructure Security"<br>• Security of Key Infrastructure Systems<br>• Defending Critical Infrastructure from Threats |

| | |
|---|---|
| | • Infrastructure Security and Resilience Measures<br>• Ensuring Resilient Critical Infrastructure Security<br>• Hardening Critical Systems Against Threats |
| **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Module overview**<br>*High-level module overview* | All aspects of Critical Infrastructure Security that includes different perspectives: technology, policy, and legal. |
| **Module description**<br>*Indicates the main purpose and description of the module.* | Definition and characteristics of Critical Infrastructures (CIs) together with their information systems will be identified, and common threats and vulnerabilities of the CI technologies (ICT/IT and OT) will be assessed and estimated based on existing standards and methodologies. |
| **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | KA1 - Cybersecurity Management<br>KA2 - Human Aspects of Cybersecurity<br>KA3 - Cybersecurity Risk Management<br>KA4 - Cybersecurity Policy, Process, and Compliance<br>KA5 - Network and Communication Security<br>KA6 - Privacy and Data Protection<br>KA7 - Cybersecurity Threat Management |
| **Category(s) of capabilities** | Refer and check D4.1. |

| | | |
|---|---|---|
| | *Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | |
| | **Learning outcomes and targets**<br>*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, participants will have gained the following:<br>**Knowledge:**<br>• Acquire a comprehensive understanding of the strategies, and best practices involved in securing critical infrastructure systems against various threats and vulnerabilities.<br>• Acquire a comprehensive understanding of the main security and resilience challenges for the protection 24/7 of critical infrastructures, considering the diverse involved perspectives (technological, policy and legal).<br>• Knowledge of the most common vulnerabilities and particular threats to Critical Infrastructures, considering the drawbacks of maintaining legacy devices (and their protocols) and the real-time performance condition.<br>• Know how to interpret relationships between CIs and the effects that may cause threats, as well as identify possible risks and their management to establish governance, security, and resilience.<br>• Knowledge of the most current regulations and normatives associated with the CIs and their specific application sectors, as well as conduct and ethical criteria.<br>**Skills:**<br>• Identify essential services, threats and possible risks in a CI or between CIs.<br>• Visualise, interpret, and analyse relations and cascading effects to compute possible risks.<br>• Identify, adapt, configure, and deploy protection solutions/technologies to provide 24/7 real-time performance and operational guarantees.<br>• Create trustworthy environments, not only for the end user, but also between CIs, |

| | | |
|---|---|---|
| | | considering the need for situational awareness and resilience.<br>• Identify and apply standards, recommendations, and best practices, but also legal, social and privacy criteria.<br>**Competencies:**<br>• Know how to identify possible misconfigurations or errors in IT and OT devices and (industrial) communication protocols that may lead to significant security risks.<br>• Lead the design, configuration, and deployments of secure and resilient CIs.<br>• Know how to support organizations in implementing measures to harden their systems, ensuring the robustness and resilience of their critical infrastructures against potential and specific threats.<br>• know the existing security technologies, mechanisms, and protocols (of TCP/IP - related to module 4 of the CSP), useful to protect communications between IT-OT components within a CI or between CIs.<br>• Know how to apply standards, recommendations, and best practices, but also legal, social and privacy criteria. |
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Introduction to Critical Infrastructure Security<br>• Sector-Specific Security Challenges<br>• Risk Assessment and Mitigation Strategies<br>• Security Controls, Resilience and Best Practices<br>• Interdependencies among Critical Infrastructures and Cascading Effects<br>• Security and risk for industrial control systems<br>• Incident Response and Recovery<br>• Regulations and Standards, including Privacy, Ethical, Legal, and Social Implications |

| | | |
|---|---|---|
| | | • Advanced Topics in Critical Infrastructure Security |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Management/ Logistics** | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Basic IT training (or) EU Digital Competence (DigComp) Framework level know-how |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | • Chief Information Security Officer (CISO)<br>• Cyber Threat Intelligence Specialist<br>• Cybersecurity Architect<br>• Cybersecurity Auditor<br>• Cybersecurity Risk Manager<br>• Cybersecurity Researcher<br>• Cybersecurity Educator |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |

| | | |
|---|---|---|
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | **Knowledge-based assessments**: As mentioned above, this type of assessment allows trainers to measure the level of knowledge received during the training phase. The assessment can be carried out in a variety of ways, such as through multiple-choice questions or tests, essay questions, or fill-in-the-blank questions.<br>In fact, frequent tests may be planned in which participants could, for example, search the web, open their textbooks, look things up easily. Tests are not to make participants fail and stress them, but to make them remember and recall knowledge and skills. That is why they should be frequent and with all sources available, where trainers may also give hints during tests if some of the participants do not understand the test questions or the purpose of the question.<br>**Performance-based assessments**: Depending on the theoretical contents, assessment may require measuring the level of participants' ability to apply practical skills, the degree of research and knowledge learned. Therefore, these evaluations can be managed in a variety of ways, such as through practical exercises, simulations or case studies. |

| | | |
|---|---|---|
| | | **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cybersecurity. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews.<br>**Behavioural assessments**: These assessments measure the participant's actual behaviour in relation to cybersecurity and their active implication during the training phase. Thus, this evaluation can be carried out in a variety of ways, such as through observation, self-report, peer-report, use of resources (e.g., forums) and regular access to the DCM platform. |

### 3.8.3 Syllabus of Training Module 8: Critical Infrastructure Security

Table 21: Critical infrastructure security: Training Module 8 syllabus.

| Main topics | Suggested content |
|---|---|
| **Introduction to Critical Infrastructure Security** | • Definition, scope, and importance of critical infrastructure.<br>• Critical infrastructure sectors and examples (energy, transportation, water, etc.)<br>• Interdependencies between various critical systems<br>• Overview of national and international security frameworks.<br>• Global threat landscape and its impact on critical infrastructure. |
| **Common Security Weaknesses and Threat Landscape** | **Most Common Security Weaknesses in Critical Infrastructure**: The deployment of new technologies and the adoption of new IT paradigms, such as Industry 4.0/5.0 and simulation, bring with them numerous security issues, especially those related to "legacy" devices and protocols. This means that the number of vulnerabilities may increase significantly, as well as the risks of their exploitation. Learners must therefore understand the major drawbacks that new IT brings to operational ecosystems, and the consequences that this in turn entails.<br>**Threat Landscape**: Classify and model attacker types and specific interests; Categorise potential threats to critical infrastructure, such as APTs or supply chain attacks, and associate those that are more targeted to specific types of critical infrastructure. |
| **Cascading Effects and Risk Assessment** | **Relations and Interdependencies**: Identify dependencies and interdependencies between Critical Infrastructures and establish levels of priority and criticality, to subsequently compute consequences between affected assets, services and users, as well as other critical infrastructures and their essential services.<br>**Visualisation of the Cascading Effect**: Model the relationships between infrastructures and their services to subsequently visualise and analyse the exploits of cascading effects between or among CIs, including the effects they might have on their own IT-OT layers. This will allow learners to have a clearer understanding of the problem and prepare contingency and |

| Main topics | Suggested content |
|---|---|
| | recovery plans for resilience.<br>**Risk Management and Assessment**: Identify threats and possible risks; Understanding cyber, physical, and natural threats; Risk Management and risk assessment through well-known methodologies, applied to critical systems. |
| **Regulations and Standards** | Regulations and Standards: Overview of regulatory frameworks and standards (e.g., NIST, ISO, ENISA, ETSI guidelines); and compliance requirements for critical infrastructure security. |
| **Security and Resilience** | **Cybersecurity for Critical Infrastructures**: Cyber threats to critical systems; Network security, including encryption, perimeter defence (equivalent to CSP Module 4), advanced intrusion detection; coordinated and advanced incident response; (dynamic) recovery against potential cyber-attacks; and situational awareness and sharing data through Cyber Threat Intelligence.<br>**Security and Resilience (including Safety)**: Risk treatment plan and Security Policy; Disaster Recovery Plan; and Business Continuity Plan. |
| **Privacy, Ethical, Legal, and Social Implications** | Ethical, Legal, and Social Implications: Ethical considerations in critical infrastructure security; Legal aspects and privacy concerns; and social impacts and community resilience. |
| **Interdependencies among Critical Infrastructures and Cascading Effects** | • Discussing the different types of dependencies among critical infrastructures, including their identification and characterisation<br>• Introducing the concept of cascading effects and highlighting examples from the literature and from practice<br>• Describing an abstract model for the cascading effects of a threat on an individual critical infrastructure |
| **Security and risk for industrial control systems** | • Principles, methods and benefits of segmenting networks in ICS environments<br>• Dividing an ICS network into separate zones or segments to limit traffic, control access and minimize the impact of attacks.<br>• Concepts, methods and best practices for implementing authentication and authorization mechanisms.<br>• Analysis of case studies and scenarios to illustrate the benefits and challenges of network segmentation |
| **Security Standards for Critical Infrastructure** | • Overview of relevant security standards for establishing a secure critical infrastructure<br>• Concepts for a critical infrastructure with a strong foundation for cybersecurity |

## 3.9 Module 9 - Software Security

This CSP training module dives deep into the essential principles and practices of software security. Participants will gain hands-on experience identifying, understanding, and mitigating software vulnerabilities throughout the development lifecycle. Through rich materials, exercises, and code reviews, the module equips individuals with the necessary skills to build secure and resilient software applications.

### 3.9.1 Target Audience and Goals

This module is designed for IT professionals, security professionals, and business leaders who need to understand the subject.

**Target Audience:**

- Developers and engineers (front-end, back-end, mobile)
- Software security professionals (analysts, pentesters, auditors)
- IT professionals responsible for secure software development (security architects, DevOps engineers)
- Product managers and business stakeholders seeking to understand software security risks.

**Goals:**

- Raise awareness of common software vulnerabilities and their impact.
- Understand secure coding practices and secure software development methodologies.
- Learn techniques for static and dynamic analysis of software for vulnerabilities.
- Gain hands-on experience with secure coding tools and best practices.
- Develop skills for threat modelling and risk assessment in software development.
- Effectively communicate software security risks and mitigation strategies to stakeholders.

### 3.9.2 Description of Training Module 9: Software Security

This CPS advanced module delves into the intricacies of software security, building upon foundational cybersecurity knowledge. It provides participants with specialized skills and strategies for securing software throughout its entire lifecycle, from design and development to deployment and maintenance.

Table 22: Software security: Training Module 9 description.

| **CSP Module Elements** | **CSP Module [field legend]** | **CSP Module Information** |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | **CSP009** |
| **Content** | **Module title**<br>*The Title of the training module* | **Software Security** |
|  | **Alternative title(s)** | • Foundations of Software Security<br>• Secure Coding Practices |

| | |
|---|---|
| *Used alternative titles for the same module by many institutes and training providers* | • Secure Software Development<br>• Cybersecurity in Software Engineering<br>• Software Security: Threats and Mitigations<br>• Security-by-Design<br>• Secure Software Engineering |
| **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Module overview**<br>*High-level module overview* | This CSP delves into the intricacies of software security, building upon foundational cybersecurity knowledge. It provides students with specialized skills and strategies for securing software throughout its entire lifecycle, from design and development to deployment and maintenance. |
| **Module description**<br>*Indicates the main purpose and description of the module.* | This CSP training module dives deep into the essential principles and practices of software security. Participants will gain hands-on experience identifying, understanding, and mitigating software vulnerabilities throughout the development lifecycle. The participants will gain in-depth knowledge of secure coding, secure software development methodologies, threat modelling, risk assessment, and security architecture, equipping them to build and maintain secure software throughout its lifecycle. Through rich materials, exercises, and code reviews, the module equips individuals with the necessary skills to build secure and resilient software applications. |
| **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance* | Diverse topics from many KAs, especially KA1, KA8, and KA9. |

| | |
|---|---|
| *KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | |
| **Category(s) of capabilities**<br>*Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | Refer and check D4.1. |
| **Learning outcomes and targets**<br>*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, participants will gain the following:<br>**Knowledge:**<br>• In-depth understanding of common software vulnerabilities and their attack vectors (e.g., injection, XSS, CSRF, memory corruption).<br>• Solid grasp of secure coding principles and best practices in various programming languages.<br>• Knowledge of secure software development methodologies like Secure SDLC and OWASP Top 10.<br>• Understanding of static and dynamic analysis tools and techniques for vulnerability detection.<br>• Awareness of security architecture principles and their application in software design.<br>• Knowledge of risk assessment methodologies for software applications.<br>• Understanding of emerging trends and challenges in software security (e.g., IoT, cloud, blockchain).<br>**Skills:**<br>• Apply secure coding practices in various programming languages to write secure and resilient code.<br>• Perform static and dynamic analysis of software applications using industry-standard tools. |

| | | |
|---|---|---|
| | | • Conduct threat modelling and risk assessment for software systems and applications.<br>• Develop and implement security architectures for secure software design.<br>• Effectively communicate software security risks and mitigation strategies to developers and stakeholders.<br>• Utilise secure coding frameworks and libraries to simplify secure coding practices.<br>• Stay informed about evolving software security threats and mitigation techniques.<br>• Hands-on experience with secure coding tools, vulnerability scanning tools, and penetration testing tools.<br>**Competencies:**<br>• Critical thinking and problem-solving in complex software security scenarios.<br>• Ability to analyse code, identify vulnerabilities, and propose effective mitigation strategies.<br>• Strong analytical and technical skills to understand and apply various security tools and techniques.<br>• Effective communication and collaboration skills to work with developers and stakeholders on security issues.<br>• Adaptability and continuous learning to stay updated with the evolving software security landscape.<br>• Ability to prioritise risks and make informed decisions regarding software security measures.<br>• Leadership potential in promoting a culture of security within software development teams. |
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Introduction to Software Security<br>• Secure Coding Practices<br>• Secure Software Development Lifecycle (SDLC)<br>• Secure Software Testing- Static and Dynamic Analysis |

| | | |
|---|---|---|
| | | • Secure Software Architecture, Deployment, Operations and Risk Management<br>• Advanced Software Security Topics<br>• Practical and Hands-on Exercises |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Management/ Logistics** | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Basic IT training (or) EU Digital Competence (DigComp) Framework level know-how |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | Cybersecurity Implementer |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Recommended ECTS** | Check online in CyberSecPro DCM System for current information on the specific module |

| | | |
|---|---|---|
| | *If applicable, the number of ECTS.* | instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | *Check online in CyberSecPro DCM System for current information on the specific module instantiation.* |

### 3.9.3 Syllabus of Training Module 9: Software Security

Table 23: Software security: Training Module 9 syllabus.

| Main topics | Suggested content |
|---|---|
| **Introduction to Software Security** | • Security concepts and principles in the context of software development.<br>• Impact of insecure software on individuals, organizations, and society.<br>• Legal and regulatory aspects of software security. |
| **Secure Coding Practices** | • Secure coding principles and best practices in specific programming languages (e.g., C, C++, Java, Python).<br>• Memory management vulnerabilities and mitigation strategies.<br>• Input validation and sanitisation techniques.<br>• Cryptography and secure coding libraries. |
| **Secure Software Development Lifecycle (SDLC)** | • Secure requirements engineering and threat modelling.<br>• Secure coding practices throughout the development process.<br>• Code reviews and security testing methodologies. |

| Main topics | Suggested content |
|---|---|
| | • Integration of security into agile development methodologies. |
| **Secure Software Testing- Static and Dynamic Analysis** | • Static code analysis tools and techniques for vulnerability detection.<br>• Dynamic application security testing (DAST) tools and methodologies.<br>• Web application security testing (WAST) and mobile application security testing (MAST).<br>• Interpreting and prioritising security test results. |
| **Secure Software Architecture, Deployment, Operations and Risk Management** | • Secure system design principles and architectures.<br>• Threat modelling frameworks and tools.<br>• Risk assessment methodologies for software applications.<br>• Implementing security controls and mitigation strategies.<br>• Software supply chain security and vulnerability management. |
| **Advanced Software Security Topics** | • Secure coding in specific application domains (e.g., IoT, cloud, blockchain).<br>• Secure coding frameworks and libraries.<br>• Software security incident response and recovery procedures.<br>• Emerging trends and challenges in software security. |
| **Practical and Hands-on Exercises** | • Applying secure coding practices in real-world coding exercises.<br>• Performing static and dynamic analysis of vulnerable software examples.<br>• Developing a security architecture and threat model for a specific application.<br>• Conducting a hands-on software security audit. |

## 3.10 Module 10 - Penetration Testing

This intensive training module provides comprehensive hands-on experience with penetration testing methodologies and tools. Participants will learn to ethically discover and exploit vulnerabilities in various IT systems, simulating real-world attacker techniques to identify and mitigate security risks. The module equips individuals with the skills and knowledge needed to conduct effective penetration testing engagements through immersive labs, exercises, and scenario-based simulations.

### 3.10.1 Target Audience and Goals

This module is designed for IT, security professionals, and anyone who needs to understand penetration testing.

**Target Audience:**

- IT security professionals (security analysts, engineers, auditors).
- Network administrators seeking to bolster security posture.
- Aspiring penetration testers wanting to enter the cybersecurity field.

**Goals:**

- Gain a solid understanding of penetration testing principles and methodologies.
- Plan, design, implement and execute penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures within an organisation.
- Develop skills to discover, exploit, and document vulnerabilities in networks, systems, and applications.
- Uncover vulnerabilities that affect the confidentiality, integrity and availability of ICT products.
- Learn to leverage various tools and techniques used by penetration testers (e.g., network scanning, vulnerability scanning, password cracking, social engineering).
- Practice navigating penetration testing frameworks and methodologies.

### 3.10.2 Description of Training Module 10: Penetration Testing

This module is designed for IT professionals, security professionals, and business leaders who need to learn knowledge and skills to perform ethical hacking (exposing organisations' weaknesses), gather intelligence, test, and improve security and offer protection against privilege escalation to prevent intrusions. The module aims to provide the trainee with a comprehensive understanding of penetrating testing within the cybersecurity landscape as it affects individuals and public and private organisations.

Table 24: Penetration testing: Training Module 10 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | **CSP010** |
| **Content** | **Module title**<br>*The Title of the training module* | **Penetration Testing** |
| | **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Ethical Hacking<br>• Security Assessment Testing<br>• Vulnerability Testing<br>• Red Teaming<br>• Security Audit and Testing<br>• White-Hat Hacking"<br>• Cybersecurity Penetration Testing<br>• Network Exploitation Testing<br>• Security Validation Testing<br>• Attack Simulation and Testing |
| | **Module offering type** | Check online in CyberSecPro DCM System for current information on the specific module |

| | |
|---|---|
| *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.* | instantiation, as this information is changing dynamically with every instantiation. |
| **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Module overview**<br>*High-level module overview* | This advanced course delves deep into the technical and strategic aspects of penetration testing. |
| **Module description**<br>*Indicates the main purpose and description of the module.* | The objective this module is to provide trainees with knowledge and skills for penetration testing to uncover any form of vulnerability ranging from small implementation bugs to major system design flaws resulting from coding errors, system configuration faults, design flaws or other operational deployment weaknesses. This course complements and expands upon foundational cybersecurity knowledge, preparing students for real-world security assessments and ethical hacking scenarios. |
| **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | KA9 |
| **Category(s) of capabilities**<br>*Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | Refer and check D4.1. |
| **Learning outcomes and targets**<br>*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, participants will gain the following:<br>**Knowledge:** |

| | | |
|---|---|---|
| | | • In-depth understanding of penetration testing methodologies and frameworks.<br>• Comprehensive knowledge of legal and ethical considerations for penetration testing engagements.<br>• Advanced understanding of network protocols, vulnerabilities, and exploitation techniques.<br>• Solid grasp of operating system vulnerabilities, web application security testing methodologies, and mobile application security principles.<br>• Awareness of cloud security concepts and penetration testing techniques.<br>• Knowledge of advanced penetration testing tools and scripting for automation.<br>• Understanding of social engineering techniques and their application in penetration testing.<br>• Knowledge of professional ethics and legal requirements for penetration testers.<br>**Skills:**<br>• Conduct thorough information gathering and reconnaissance using advanced tools and techniques.<br>• Perform advanced network scanning and vulnerability assessments to identify and exploit vulnerabilities.<br>• Penetrate and exploit operating systems, web applications, and mobile applications using advanced tools and techniques.<br>• Develop and execute post-exploitation strategies for maintaining access and escalating privileges.<br>• Write comprehensive and informative penetration testing reports, documenting findings and recommendations.<br>• Effectively communicate test results and vulnerabilities to both technical and non-technical audiences.<br>• Utilise scripting for automation and custom exploit development. |

| | | |
|---|---|---|
| | | • Apply ethical hacking techniques and social engineering in controlled, simulated environments.<br>**Competencies:**<br>• Critical thinking and problem-solving in complex penetration testing scenarios.<br>• Ability to analyse information, identify vulnerabilities, and develop effective exploitation strategies.<br>• Strong analytical and technical skills to utilise advanced penetration testing tools and methodologies.<br>• Effective communication and collaboration skills to work with clients and stakeholders.<br>• Adaptability and continuous learning to stay updated with evolving threats and technologies.<br>• Ability to prioritize risks, make ethical decisions, and act responsibly in penetration testing engagements.<br>• Leadership potential in planning, conducting, and reporting on penetration testing projects. |
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Introduction to Penetration Testing<br>• Advanced Information Gathering and Reconnaissance<br>• Network Penetration Testing<br>• System and Application Penetration Testing<br>• Essentials of Encryption<br>• Advanced Penetration Testing Tools and Techniques<br>• Development and Delivery of Reports<br>• Ethics and Professionalism in Penetration Testing |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |

| | | |
|---|---|---|
| Management/ Logistics | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Basic IT training (or) EU Digital Competence (DigComp) Framework level know-how |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | • Penetration Tester (PENT)<br>• Vulnerability Assessment and Penetration Testing Specialist (VAPTS)<br>• Cybersecurity Incident Responder (CSIR) |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module |

| | | |
|---|---|---|
| | | instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | *Check online in CyberSecPro DCM System for current information on the specific module instantiation. Some of the aspects considered are listed below:*<br>Have the participants achieved the learning outcomes if they succeeded in a final test on AIS jamming and spoofing specificities? |

### 3.10.3 Syllabus of Training Module 10: Penetration Testing

Table 25: Penetration testing: Training Module 10 syllabus.

| Main topics | Suggested content |
|---|---|
| **Introduction to Penetration Testing** | • Penetration testing concepts, methodologies, and frameworks: Planning and preparation for penetration testing, penetration testing procedures, penetration testing standards, methodologies and frameworks, penetration testing tools.<br>• Legal and ethical considerations for penetration testing engagements.<br>• Planning and scoping penetration testing engagements.<br>• Client communication and documentation best practices. |
| **Advanced Information Gathering and Reconnaissance** | • Advanced OSINT techniques (social media, public records, data breaches).<br>• Network reconnaissance and foot printing strategies.<br>• Utilizing advanced information gathering tools (i.e., Maltego, SpiderFoot).<br>• DNS, Web reconnaissance |
| **Network Penetration Testing** | • Advanced network scanning and vulnerability assessment methodologies.<br>• Exploiting network vulnerabilities with advanced tools (Metasploit, Nmap NSE scripts).<br>• Wireless network penetration testing (802.11 attacks, wireless intrusion detection/prevention systems). |

| Main topics | Suggested content |
|---|---|
| | • Post-exploitation techniques for maintaining access and privilege escalation.<br>• TCP, UDP connections, scanning |
| **System and Application Penetration Testing** | • Operating system penetration testing (Windows, Linux) with advanced tools (i.e., Mimikatz, PowerSploit).<br>• Web application security testing (OWASP Top 10, SQL injection, XSS, CSRF).<br>• Mobile application security testing (static and dynamic analysis tools).<br>• Cloud security testing concepts and techniques.<br>• Databases, SQL injection, Web authentication and session management, Browser proxies and non-rendered content, cross-site scripting, HTTP, JavaScript, and command injection |
| **Essentials of Encryption** | • Wireless networks and encryption, lock picking, master keys, and oracle hacks, cryptography weaknesses, SSL and TLS encryption, digital signatures |
| **Advanced Penetration Testing Tools and Techniques** | • Scripting for automation and custom exploitation.<br>• Social engineering techniques and tools for physical and virtual environments.<br>• Advanced privilege escalation techniques and bypassing security controls.<br>• Cloud penetration testing tools and platforms. |
| **Development of reports** | • Vulnerability assessment results report, penetration testing report |
| **Ethics and Professionalism in Penetration Testing** | • Conducting penetration testing engagements on simulated real-world scenarios.<br>• Applying learned techniques to exploit vulnerabilities in virtualized environments.<br>• Writing comprehensive penetration testing reports based on lab exercises.<br>• Critically analysing real-world penetration testing case studies. |

## 3.11 Module 11 - Cyber Ranges and Operations

This immersive CSP training module delves into the practical world of cyber ranges and operations. Participants will gain hands-on experience navigating simulated cyber environments, deploying countermeasures, and responding to real-world attack scenarios. Aligned with industry best practices, the module equips individuals with the skills and knowledge needed to effectively operate and utilise cyber ranges for training, testing, and research purposes.

### 3.11.1 Target Audience and Goals

This module is designed for IT professionals, security professionals, and business leaders who need to understand the subject.

**Target Audience:**

- Cybersecurity professionals (incident responders, analysts, threat hunters).
- Network administrators and engineers seeking to bolster security posture.
- Students aspiring to enter the cybersecurity field.
- Individuals seeking certification in cyber range operations (e.g., CRISC).

**Goals:**

- Master the fundamentals of cyber ranges and their role in cybersecurity training and testing.
- Gain hands-on experience navigating various types of cyber range environments (virtual, cloud-based).
- Develop skills in deploying security controls, analysing network traffic, and identifying attack indicators.
- Practice incident response procedures and containment strategies in simulated scenarios.
- Learn to build, configure, and manage cyber range platforms for different use cases.
- Understand best practices for cybersecurity exercises, assessments, and research within cyber ranges.
- Prepare for industry certifications related to cyber range operations.

### 3.11.2 Description of Training Module 11: Cyber Ranges and Operations

This module is designed for IT professionals, security professionals, and business leaders who need to learn this subject. This immersive CSP module delves into the intricacies of cyber ranges and operations, aligning with leading industry best practices. The participants will gain hands-on experience in simulated cyber environments, developing the skills and knowledge needed to design, manage, and utilise cyber ranges for effective training, testing, and research purposes. This module complements and expands upon foundational cybersecurity knowledge, preparing students for real-world cybersecurity exercises and incident response scenarios.

Table 26: Cyber ranges and operations: Training Module 11 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | **CSP011** |
| **Content** | **Module title**<br>*The Title of the training module* | **Cyber Ranges and Operations** |
| | **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Offensive Practices<br>• Defensive Practices<br>• Hands-on Cybersecurity Training<br>• Computer and Network Security in Practice |

| | |
|---|---|
| **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Module overview**<br>*High-level module overview* | Advanced hands-on network security educational scenario, including simulated cyber environments, deploying countermeasures, and responding to real-world attack scenarios. |
| **Module description**<br>*Indicates the main purpose and description of the module.* | Aligned with industry best practices, the module equips individuals with the skills and knowledge needed to effectively operate and utilise cyber ranges for training, testing, and research purposes. The current network security educational scenario is an interdisciplinary activity requiring background from various courses such as Computer networks, databases and Web programming. The scenario can be executed collaboratively or competitively, in which case there will be two antagonistic teams: the blue team (defenders) and the red team (attackers). The trainees will assume various roles during the scenario, such as network engineers, administrators, users, and attackers. |
| **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management*<br>*KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | Combination of KA5, KA8, KA9 and KA10<br>*KA5 – Network and Communication Security*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* |
| **Category(s) of capabilities** | Refer and check D4.1. |

| | | |
|---|---|---|
| | *Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | |
| | **Learning outcomes and targets**<br>*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, participants will gain the following:<br>**Knowledge:**<br>• In-depth understanding of various types of cyber ranges and their applications (virtual, cloud-based, hardware-based).<br>• Solid grasp of industry best practices and standards for cyber range operations.<br>• Gain interdisciplinary knowledge from Computer networks, databases, and Web programming.<br>• Comprehensive knowledge of ethical considerations and responsible use of cyber ranges.<br>• Understanding of cybersecurity frameworks and methodologies utilised in cyber range exercises (incident response, vulnerability assessment).<br>• Awareness of emerging trends and future directions in cyber range technology.<br>• Knowledge of security best practices for managing and maintaining cyber range environments.<br>• Understanding of data backup, recovery, and disaster planning in cyber range contexts.<br>**Skills:**<br>• Navigate and utilise simulated cyber environments with proficiency.<br>• Deploy and configure security controls, firewalls, and intrusion detection/prevention systems.<br>• Analyse network traffic to identify indicators of compromise (IOCs) and respond to simulated cyberattacks.<br>• Develop and execute incident response playbooks and containment strategies within controlled environments.<br>• Design and configure basic cyber range exercises using industry-standard frameworks (e.g., MITRE ATT&CK). |

| | | |
|---|---|---|
| | | • Evaluate and utilise various cyber range platforms for different use cases (training, vulnerability testing, research).<br>• Build and utilise basic custom cyber range tools and scripts for automation and enhanced analysis.<br>• Effectively communicate findings and lessons learned from cyber range exercises.<br>**Competencies:**<br>• Critical thinking and problem-solving in complex cyber range scenarios.<br>• Ability to analyse network traffic, identify malicious activity, and make informed decisions during simulated incidents.<br>• Adaptation and continuous learning to stay updated with evolving cyber threats and best practices.<br>• Effective communication and collaboration skills to work with instructors, peers, and other stakeholders.<br>• Leadership potential in designing, managing, and facilitating cyber range exercises.<br>• Ability to prioritise risks, make ethical decisions, and act responsibly in cyber range operations.<br>• Competence in utilising cyber ranges for effective cybersecurity training, testing, and research purposes. |
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Introduction to Cyber Ranges and Operations<br>• Hands-on Cyber Range Exercises<br>• Cyber Range Design and Configuration<br>• Advanced Cyber Range Operations<br>• Cyber Range Management and Maintenance<br>• Special Topics in Cyber Range Operation |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |

| | | |
|---|---|---|
| Management/ Logistics | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | • Background knowledge in Computer networks, databases, and Web programming.<br>• Familiarity with basic hardware and software used in network security. |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)**<br>*An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | • Cybersecurity Educator<br>• Cybersecurity Researcher<br>• Chief Information Security Officer (CISO) |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |

| | | |
|---|---|---|
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | *Check online in CyberSecPro DCM System for current information on the specific module instantiation. Some of the aspects considered are listed below:*<br>• Assessment of ability to solve advanced cybersecurity exercises and scenarios for simulations, virtual or cyber range environments.<br>• Assessment of ability to integrate knowledge from various disciplines.<br>• Evaluation of practical skills in web application development and LAN management.<br>• Testing knowledge and skills in software installation and network configuration.<br>• Assessment of proficiency in using network traffic analysis tools.<br>• Evaluation through simulated cyber-attack exercises. |

### 3.11.3 Syllabus of Training Module 11: Cyber Ranges and Operations

Table 27: Cyber ranges and operations: Training Module 11 syllabus.

| Main topics | Suggested content |
|---|---|
| **Introduction to Cyber Ranges and Operations** | • Definition, purpose, and benefits of cyber ranges.<br>• Types of cyber ranges (virtual, cloud-based, hardware-based).<br>• Industry best practices and standards<br>• Interdisciplinary aspects of network security. |

| Main topics | Suggested content |
|---|---|
| | • Collaborative and competitive execution of scenarios in network security.<br>• Ethical considerations and responsible use of cyber ranges. |
| **Hands-on Cyber Range Exercises** | • Navigating simulated cyber environments.<br>• Deploying security controls and network infrastructure.<br>• Analysing network traffic and identifying IOCs.<br>• Responding to simulated cyberattacks and incidents.<br>• Practicing incident response playbooks and containment strategies. |
| **Cyber Range Design and Configuration** | • Selecting and configuring cyber range platforms.<br>• Designing basic cyber range exercises (attack scenarios, objectives).<br>• Integrating industry frameworks (MITRE ATT&CK) into exercises.<br>• Managing user access and permissions within the cyber range. |
| **Advanced Cyber Range Operations** | • Building and utilising custom cyber range tools and scripts.<br>• Automating incident response actions within the cyber range.<br>• Conducting vulnerability assessments and penetration testing within the range.<br>• Integrating threat intelligence and real-world attack data into exercises |
| **Cyber Range Management and Maintenance** | • Security best practices for managing cyber range environments.<br>• Data backup, recovery, and disaster planning for cyber ranges.<br>• User training and support for cyber range operations.<br>• Evaluating and reporting on cyber range exercise outcomes. |
| **Special Topics in Cyber Range Operations** | • Cloud-based cyber ranges and their unique considerations.<br>• Mobile device and IoT security testing within cyber ranges.<br>• Integrating cyber ranges with security information and event management (SIEM) tools.<br>• Emerging trends and future directions in cyber range technology. |

## 3.12 Module 12 - Digital Forensics

This advanced CSP module provides a comprehensive understanding of digital forensics principles and practices, aligning with leading industry best practices. The participants will gain in-depth knowledge of acquiring, analysing, interpreting, and presenting digital evidence from various electronic devices and platforms. This module emphasizes hands-on experience, ethical considerations, and legal aspects of digital forensic investigations, preparing trainee for real-world cybersecurity and criminal justice settings.

### 3.12.1 Target Audience and Goals

This module is designed for IT professionals, security professionals, and business leaders who need to understand the subject.

**Target Audience:**

- IT security professionals (incident responders, cybersecurity analysts).
- Law enforcement and legal professionals investigating cybercrime.
- Digital security consultants and private investigators.
- Individuals pursuing digital forensics careers.

**Goals:**

- Master the fundamental principles and methodologies of digital forensics.
- Gain hands-on experience acquiring digital evidence from various devices (computers, mobile phones, cloud storage).
- Learn to analyse and interpret diverse digital evidence formats (data carving, file system analysis, log files).
- Develop skills in preserving and documenting digital evidence with chain-of-custody procedures.
- Understand legal and ethical considerations in digital forensics investigations.
- Practice presenting digital evidence findings effectively in reports and courtroom settings.

### 3.12.2 Description of Training Module 12: Digital Forensics

This CSP module is designed for IT professionals, security professionals, and business leaders who need to understand digital forensics principles and practices, aligning with leading industry best practices.

Table 28: Digital forensics: Training Module 12 description.

| CSP Module Elements | CSP Module [field legend] | CSP Module Information |
|---|---|---|
| **Code** | *Code format: CSP001_x where x is the module offering type (see below) and it(_x) will be included in sector-specific offering syllabus in D3.3(health), D3.4(energy), D3.5(maritime)*<br>*The purpose of this format is to apply the code to every place you use this module as part of the CSP programme.*<br>*The Generic Model Syllabi as a simple code, as seen in the next column.* | **CSP012** |
| **Content** | **Module title** | **Digital Forensics** |

| | |
|---|---|
| *The Title of the training module* | |
| **Alternative title(s)**<br>*Used alternative titles for the same module by many institutes and training providers* | • Cyber Forensics<br>• Computer Forensics<br>• Digital Investigation and Analysis<br>• Electronic Forensics<br>• Cybercrime Forensics<br>• Forensic Computing<br>• Incident Response and Forensics<br>• Data Forensics<br>• Forensic Cybersecurity<br>• Information Forensics |
| **Module offering type**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Level**<br>*Training level: B (Basic), A (Advanced)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Module overview**<br>*High-level module overview* | The module introduces learners to digital forensics to equip them with the knowledge and skills to undertake cybercriminal investigations that produce digital evidence that may prove a malicious activity. |
| **Module description**<br>*Indicates the main purpose and description of the module.* | This module aims to build learners' capacity to conduct cybercrime investigations. It introduces the learner to digital forensics and techniques for conducting forensic examinations. The module also enables learners to examine digital evidence, including data acquisition and identification analysis and how digital evidence artefacts may enable intrusion investigation. To complement automated digital forensic tools, learners are introduced to base Python programming language, which can allow them to conduct forensic tasks such as simulation of attacks, evidence cloning, and port scanning. |
| **Knowledge Area(s)**<br>*Mapping to the 10 selected CSP knowledge areas.*<br>*KA1 – Cybersecurity Management* | KA1, KA10 |

| | | |
|---|---|---|
| | *KA2 – Human Aspects of Cybersecurity*<br>*KA3 – Cybersecurity Risk Management*<br>*KA4 – Cybersecurity Policy, Process, and Compliance*<br>*KA5 – Network and Communication Security*<br>*KA6 – Privacy and Data Protection*<br>*KA7 – Cybersecurity Threat Management*<br>*KA8 – Cybersecurity Tools and Technologies*<br>*KA9 – Penetration Testing*<br>*KA10 – Cyber Incident Response* | |
| | **Category(s) of capabilities**<br>*Indicate CSP market-oriented capabilities (e.g., cybersecurity tools and technologies)* | Refer and check D4.1. |
| | **Learning outcomes and targets**<br>*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, participants will gain the following:<br>**Knowledge:**<br>• Knowledge of digital forensics methods, best practices and tools.<br>• Knowledge of digital forensics analysis techniques.<br>• Knowledge of digital forensics testing techniques.<br>• Knowledge of criminal investigation methodologies and procedures.<br>• Knowledge of malware analysis tools.<br>• Knowledge of cyber threats and vulnerabilities.<br>• Advanced knowledge of cybersecurity attack tactics and techniques.<br>• Knowledge of legal framework related to cybersecurity and data protection.<br>• Knowledge of operating systems security<br>• Computer network security.<br>**Skills:**<br>• Work ethically and independently without bias. |

| | | |
|---|---|---|
| | | • Retrieve information while preserving its integrity.<br>• Identifying, analysing, and correlating cybersecurity events.<br>• Maintain chain-of-custody procedures to ensure the admissibility of digital evidence.<br>• Conduct network forensics investigations and analyse network traffic logs for malicious activity.<br>• Extract and analyse digital evidence from mobile devices (Android, iOS).<br>• Visualize complex digital forensic data for clear communication in various settings.<br>• Report and present digital evidence in an understandable way.<br>• Produce a detailed and objective investigative report.<br>**Competencies:**<br>• Critical thinking and problem-solving in complex digital forensic scenarios.<br>• Ability to analyse digital evidence, identify relevant indicators, and draw sound conclusions.<br>• Attention to detail and meticulousness in handling and processing digital evidence.<br>• Effective communication and presentation skills to articulate technical findings to technical and non-technical audiences.<br>• Adaptability and continuous learning to stay updated with evolving technologies and cyber threats.<br>• Ethical decision-making and adherence to legal regulations in digital forensic investigations.<br>• Independent ability to conduct and manage digital forensic investigations from start to finish. |
| | **Main topics and contents list**<br>*A list of main topics and key content* | • Introduction to Digital Forensics<br>• Tools for Digital Forensics<br>• Data/evidence Acquisition |

| | | |
|---|---|---|
| | | - Legal Aspects of Digital Forensics<br>- Digital Forensics Analyses<br>- Programming for Digital Forensics<br>- Computing Investigation and Crime Processing<br>- Network Forensics and Incident Response<br>- Mobile Device Forensics<br>- Digital Forensics Reporting and Presentation<br>- Advanced Topics in Digital Forensics |
| | **Language**<br>*Indicates the spoken language and the language for the material and the assessment/evaluation* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Management/ Logistics** | **Training Provider**<br>*Name(s) of training providers.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Contact**<br>*Name(s) of the main contact person and their email address.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Dates offered**<br>*Indicates the semester / specific dates for the schedule of the training, as well as periodicity (e.g., even after the end of the CSP programme).* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Duration**<br>*Duration of the training.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Training method and provision**<br>*Indicates Physical, Virtual, or Both. If physical, provide details about the location. If virtual, provide the URL link of the website.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Pre-requisites** | Basic IT training (or) EU Digital Competence (DigComp) Framework level know-how |
| | **Relevance to European Cybersecurity Skills Framework (ECSF)** | - Digital Forensics Investigator<br>- Cyber Incident Responder |

| | | |
|---|---|---|
| | *An indicative relevance of this module training with ECSF. It also indicates which ECSF profiles need this module.* | |
| | **Tools to be used**<br>*A list of tools that will be used for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Recommended ECTS**<br>*If applicable, the number of ECTS.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Certificate of Attendance (CoA)**<br>*Indicates Yes or No (even in case of partial attendance)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Module enrolment dates**<br>*Indicates the enrolment dates for the operation of this training module.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Other important dates**<br>*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.* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| **Outcomes** | **Evaluation method(s)**<br>*Method for the evaluation of the learner's performance (indicates physical and/or virtual tests, participation, exercises, etc.)* | Check online in CyberSecPro DCM System for current information on the specific module instantiation, as this information is changing dynamically with every instantiation. |
| | **Evaluation and verification of learning outcomes**<br>*Assessment elements and high-level process to determine participants have achieved the learning outcomes* | *Check online in CyberSecPro DCM System for current information on the specific module instantiation. Some of the aspects considered are listed below:*<br>**Knowledge-based assessments**: These assessments measure the participant's knowledge of the material covered in the training. They can be administered in various ways, such as through multiple-choice, essay, or fill-in-the-blank questions.<br>**Performance-based assessments**: These assessments measure the participant's ability to apply the skills and knowledge they learned in the training. They can be administered in various ways, such as through practical exercises, simulations, or case studies. |

| | | |
|---|---|---|
| | | **Attitudinal assessments**: These assessments measure the participant's attitudes and beliefs about cybersecurity. They can be administered in a variety of ways, such as through surveys, questionnaires, or interviews.<br>**Behavioural assessments**: These assessments measure the participants' actual behaviour in relation to cybersecurity. They can be administered in various ways, such as through observation, self-report, or peer-report. |

### 3.12.3 Syllabus of Training Module 12: Digital Forensics

Table 29: Digital forensics: Training Module 12 syllabus.

| Main topics | Suggested content |
|---|---|
| **Introduction to Digital Forensics** | • Understand the fundamentals of general forensic science and digital forensics.<br>• Benefits of digital forensics.<br>• Digital forensics process. |
| **Tools for Digital Forensics** | • Hardware and software tools.<br>• Tools selection and validation.<br>• Digital forensics quality assurance |
| **Data/evidence acquisition** | • Understanding data storage formats and digital evidence.<br>• Acquisition tools and determination of best acquisition methods.<br>• Validation of data acquisitions. |
| **Legal aspects of digital forensics** | • Understanding the legal aspects of digital forensics and their impact on digital forensics |
| **Digital forensics analyses** | • Malware analysis.<br>• Volatile memory analysis.<br>• Timeline analysis.<br>• Intrusion analysis. |
| **Programming for digital forensics** | • Understanding Python programming for digital forensics.<br>• Use of Python base programming for performing tasks such as simulation of attacks, port scanning, website cloning, load generation and testing of a website, wireless network scanning, transmission of traffic in the network, etc. |
| **Computing investigation and crime processing** | • Digital forensics process model: Introduction to cyber-crime scenes.<br>• Scene and evidence documentation.<br>• Chain of custody.<br>• Forensic evidence cloning.<br>• Integrity of evidence; reporting |

| Main topics | Suggested content |
|---|---|
| **Network Forensics and Incident Response** | • Investigating network intrusions and cyberattacks through digital evidence analysis.<br>• Log file analysis and network traffic capture techniques.<br>• Incident response procedures and evidence collection in cybercrime scenarios. |
| **Mobile Device Forensics** | • Acquisition and analysis of digital evidence from mobile devices (Android, iOS).<br>• Mobile forensics tools and techniques for extracting data and applications.<br>• Analysing call logs, text messages, and social media activity. |
| **Digital Forensics Reporting and Presentation** | • Writing comprehensive digital forensic reports, documenting findings and analysis.<br>• Presenting digital evidence effectively in court, legal proceedings, and technical settings.<br>• Visualizing complex digital forensic data for clear communication. |
| **Advanced Topics in Digital Forensics** | • Cloud forensics and investigating evidence stored in cloud platforms.<br>• Emerging trends and challenges in digital forensics (cybercrime evolution, IoT forensics) |

## 3.13 Analysis of Interrelationships between Module Components

This section analyses the interrelationships between the CyberSecPro programme module components to justify how they address the prioritised knowledge areas in deliverable D2.3, the CyberSecPro market-oriented capabilities, and ENISA's ECSF.

Part of the development work in CyberSecPro Work Package 2 culminated in deliverable D2.3, which analysed and prioritised cybersecurity knowledge areas within the scope and context of CyberSecPro's education and training programme. The provisioning of these knowledge areas considered a) the cybersecurity professional market analysis provided in deliverable D2.1, b) their relevance to the ECSF, c) the availability of resources at CyberSecPro partners' institutions as analysed and determined in deliverable D2.2, and d) their general significance and alignment with established CyberSecPro market-oriented capabilities. The criteria followed in analysing and prioritising the knowledge areas acknowledge and take into cognisance the significance and interplay between identified skills gaps, ECSF and cybersecurity market-oriented capabilities.

In addition to prioritising knowledge areas based on the criteria mentioned above and aiming to bridge the gaps in cybersecurity workforce skills development, D2.3 also established an initial set of cybersecurity modules that target the prioritised knowledge areas. To select the modules, course offerings provided by CyberSecPro partners were thoroughly reviewed via evaluation and mapping against the knowledge areas of priority to ensure they fit for purpose. The selection process further ensured 1) the identification of cybersecurity modules that covered the prioritised knowledge areas, 2) there was no duplication of effort within CyberSecPro, 3) the leveraging of resources and workforce within the consortium, and 4) the avoidance of redundancy and fostering synergy within the consortium. Because the module selection targeted the prioritised cybersecurity knowledge areas, the criteria for cybersecurity knowledge prioritisation is subsumed in the selected modules. Therefore, the selected modules are deemed to address skill gaps, cybersecurity market-oriented capabilities, and the ECSF.

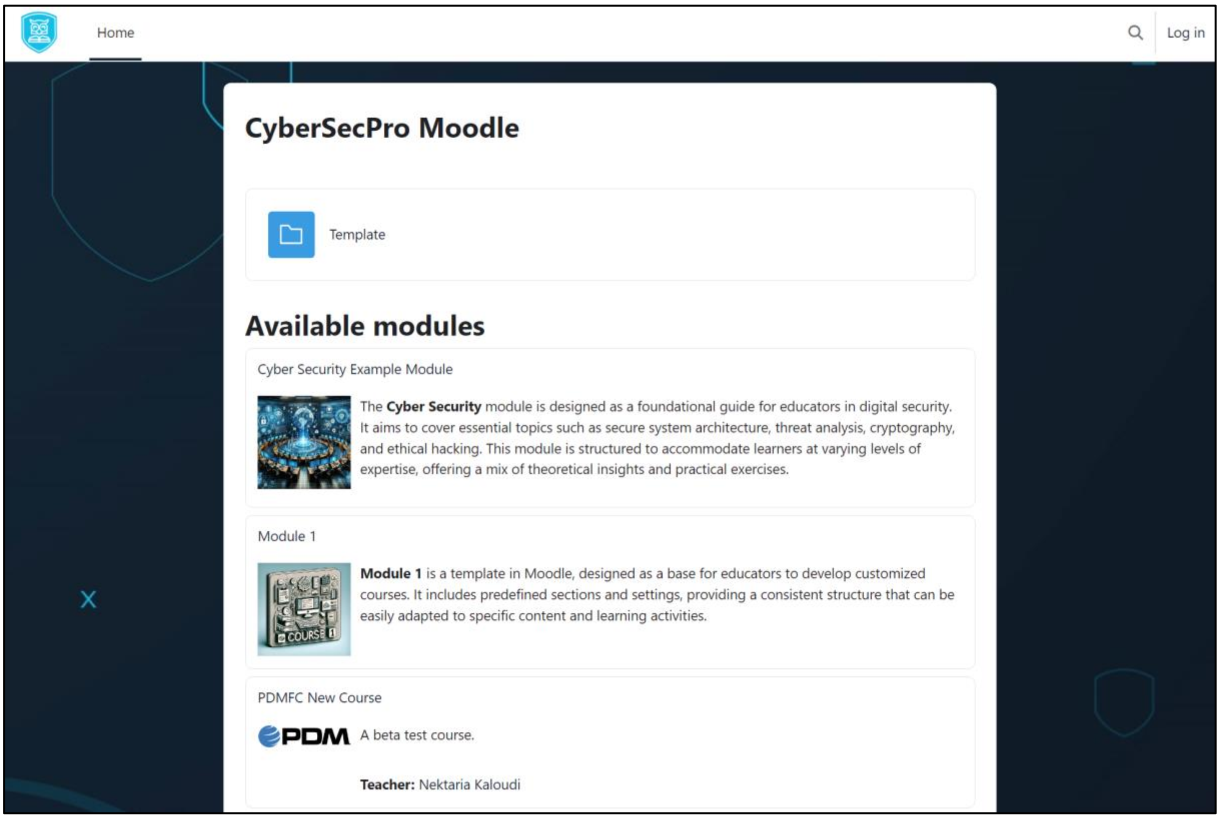
It is important to re-emphasise that one of CyberSecPro's main goals is to enhance the cybersecurity programmes offered across the EU, starting with programmes offered by CyberSecPro partners to bridge the skilled workforce gap. Following the foundation and thrust of early CyberSecPro deliverables, especially D2.3, the current deliverable D3.1 has provided 12 core cybersecurity modules targeting the prioritised knowledge areas. These 12 core modules were designed, and their corresponding syllabuses were developed following the criteria for prioritising knowledge and selection of modules in D2.3 highlighted in previous paragraphs. It is essential to mention that the specified curriculum and syllabuses for each of the three key sectors considered in CyberSecPro are developed based on the core curriculum template. The core modules and their corresponding curriculum template and syllabuses serve as the basis for CyberSecPro's operational plan for the training as provided in D4.1.

In order to further analyse interrelationships between key module components, we consider the cybersecurity curriculum template defined for any of the core modules in this deliverable. The template captures the fundamental module components, including the cybersecurity knowledge areas, relevance to ECSF, and market-driven cybersecurity capabilities. The process of designing the curriculum of each core cybersecurity module and its corresponding syllabus makes it mandatory to ascertain explicitly: 1) the prioritised knowledge areas(s) fulfilled by the module, 2) the CyberSecPro market-driven capability(s) fulfilled by the module, and 3) the module's relevance to the ECSF. In addition to complying with these mandatory specifications, achieving the learning outcomes and targets defined in the module's curriculum ensures that trainees graduate with the required cybersecurity workforce skills.

# 4 CyberSecPro DCM Setup

The CyberSecPro DCM needs to use a reliable DCM system to adapt to the 21st-century constantly changing cybersecurity market needs and to accomplish project SO4.3 – “*Use a reliable, dynamic Curriculum Management System to adapt to a 21st-century constantly changing cybersecurity market needs; be agile and responsive to changing curricula needs*”. As discussed in D2.3, the constraints and requirements for adopting the CyberSecPro programme have been analysed, encompassing business, technical, legal, social, and financial barriers. Solutions to overcome these barriers have been presented, emphasising the need for strategic planning, effective communication, and persistent efforts. These findings help anticipate and address potential blockages in the programme's implementation, achievement, and validation.

The assessment criteria for the DCM system selection were established, and available systems on the market were evaluated accordingly. The chosen system was Moodle [42]. An analysis was conducted mapping the previously identified requirements to Moodle to uncover areas where the system already meets the requirements and areas where modifications or adaptations need to be made. This ensures that the chosen system can meet the specific needs of the CyberSecPro education and training programme. This chapter presents the selected DCM (Moodle) and its functionalities. The DCM is available through the CyberSecPro project website. Figure 4 shows the CyberSecPro DCM, accessible by all project partners, and which was parametrised according to the information provided in this chapter. The CyberSecPro DCM will be continuously updated to meet the project needs and according to the feedback received.



CyberSecPro Moodle

Template

Available modules

Cyber Security Example Module

The **Cyber Security** module is designed as a foundational guide for educators in digital security. It aims to cover essential topics such as secure system architecture, threat analysis, cryptography, and ethical hacking. This module is structured to accommodate learners at varying levels of expertise, offering a mix of theoretical insights and practical exercises.

Module 1

**Module 1** is a template in Moodle, designed as a base for educators to develop customized courses. It includes predefined sections and settings, providing a consistent structure that can be easily adapted to specific content and learning activities.

PDMFC New Course

A beta test course.

**Teacher:** Nektaria Kaloudi

Figure 4: CyberSecPro DCM screenshot.

## 4.1 Moodle Parameterisation

### 4.1.1 Background

The evolution of educational technology has reshaped the landscape of teaching and learning, bringing forth innovative platforms that cater to the dynamic needs of educators and students. In this context, Moodle stands out as a powerful and versatile Learning Management System (LMS) that has gained widespread adoption in educational institutions globally [42].

As we embark on the journey of this project, it is essential to recognize the growing significance of Moodle in modern education. Moodle serves as a repository for educational resources and a comprehensive framework for delivering courses, engaging students, and facilitating collaboration.

Educational institutions worldwide are increasingly leveraging Moodle to enhance the quality of education, streamline administrative processes, and embrace flexible teaching methodologies. The platform's open-source nature and extensive feature set make it a compelling choice for those seeking a customizable and scalable solution, supported by an extensive and growing community [43].

### 4.1.2 Objectives

The primary objectives of this project revolve around the parametrization of Moodle to align it with the specific requirements and goals of our educational institution. We aim to maximise its potential as a pedagogical tool, administrative aid, and collaborative platform by customising Moodle to our unique needs.

#### 4.1.2.1 Enhance user experience

Our foremost objective is to enhance the overall user experience for educators and students. By optimising the layout, accessibility, and functionality of Moodle, we intend to create an intuitive and user-friendly environment that fosters effective teaching and learning.

#### 4.1.2.2 Streamline administrative processes

Moodle offers a range of administrative features that can be tailored to align with our institution's administrative workflows. Our goal is to streamline course creation, user management, and reporting processes, thereby reducing administrative overhead and improving operational efficiency.

#### 4.1.2.3 Facilitate personalised learning paths

Recognizing the diverse learning needs of students, we aim to implement parametrization that allows for the creation of personalised learning paths. This involves configuring Moodle to support adaptive learning strategies, competency-based assessments, and individualised feedback mechanisms.

#### 4.1.2.4 Ensure data security and compliance

Data security and privacy are paramount in an educational environment. As part of this project, we will focus on configuring Moodle to adhere to industry best practices for data security and compliance, ensuring the confidentiality and integrity of user data.

#### 4.1.2.5 Foster collaboration and engagement

Moodle's collaborative features are central to its effectiveness. We intend to harness these features to promote collaboration and engagement among students and educators. This includes configuring discussion forums, collaboration tools, and multimedia integration to create a vibrant online learning community.

By addressing these objectives, we aim to harness the full potential of Moodle as a dynamic and adaptable educational platform. This project represents a strategic investment in our institution's digital infrastructure, aiming to provide an enriched and tailored educational experience for all stakeholders.

## 4.2 Moodle Overview

### 4.2.1 Features and Capabilities

#### 4.2.1.1 Course Management

Moodle provides a robust platform for efficient course management. Educators can easily create, organise, and deliver courses using various multimedia content. The platform supports the creation of engaging lessons, assignments, and assessments.

#### 4.2.1.2 Collaboration Tools

Fostering collaboration is a key strength of Moodle. The platform offers a suite of collaboration tools, including discussion forums, wikis, and real-time messaging. These tools enable a dynamic and interactive learning environment where students and educators can engage in meaningful discussions and collaborative projects.

#### 4.2.1.3 Assessment and Grading

Moodle streamlines the assessment process with its versatile and customizable features. Educators can create quizzes, surveys, and assignments tailored to their specific teaching methodologies. The platform also offers a comprehensive gradebook that supports efficient grading and provides valuable insights into student performance.

#### 4.2.1.4 Flexibility and Adaptability

One of Moodle's standout features is its flexibility. The open-source platform allows extensive customization to meet the unique needs of different educational institutions. This adaptability ensures that Moodle can evolve alongside changing pedagogical approaches and technological advancements.

#### 4.2.1.5 Multimedia Integration

Moodle supports multimedia integration, allowing educators to enhance their courses with videos, images, and interactive content. This multimedia capability makes learning more engaging and accommodates diverse learning styles.

#### 4.2.1.6 Accessibility

Ensuring accessibility for all users is a core principle of Moodle. The platform is designed to meet accessibility standards, making it inclusive and accommodating to learners with diverse needs.

### 4.2.2 Importance in Education

#### 4.2.2.1 Scalability

Moodle's scalability is a significant advantage for educational institutions. Whether catering to a small class or a large-scale online programme, Moodle can handle the diverse needs of educational organisations, providing a scalable solution that grows with the institution.

#### 4.2.2.2 Cost-Effectiveness

Being an open-source platform, Moodle offers a cost-effective solution for educational institutions. The absence of licensing fees makes it an attractive option for organisations looking to optimise their budgets without compromising features and functionality.

#### 4.2.2.3 Community Support

Moodle benefits from a vibrant and active community of developers, educators, and administrators. This community support ensures the platform is regularly updated, secure, and enriched with new features.

Institutions adopting Moodle become part of a global network, accessing a wealth of shared knowledge and best practices.

#### 4.2.2.4 Pedagogical Flexibility

Educators appreciate Moodle's pedagogical flexibility, allowing them to implement diverse teaching strategies. Moodle accommodates various instructional methodologies, whether following a traditional classroom model, a blended learning approach, or fully online courses.

#### 4.2.2.5 Data Security and Privacy

Moodle prioritises data security and privacy, crucial aspects in the education sector. Institutions can have confidence in protecting sensitive student and organisational data, aligning with regulatory requirements and ensuring a secure learning environment.

In summary, Moodle's rich feature set, adaptability, and cost-effectiveness make it a cornerstone in modern education. Its importance extends beyond the technical realm, contributing to educational institutions' pedagogical flexibility and overall success.

## 4.3 Scope

### 4.3.1 Defined Parameters

In order to effectively carry out the parametrization of Moodle for our institution, it is crucial to establish clear and defined parameters. These parameters will serve as the guiding principles for customization and configuration, ensuring that the modifications align with the institution's specific needs and objectives.

#### 4.3.1.1 User Roles and Permissions

One of the key parameters involves defining user roles and permissions within the Moodle ecosystem. This includes specifying the responsibilities and access levels for administrators, educators, students, and support staff. By clearly delineating these roles, we aim to create a structured and secure environment that respects privacy and data integrity.

#### 4.3.1.2 Course Structures and Taxonomies

Parametrization will extend to the configuration of course structures and taxonomies. This involves defining the hierarchy of courses, modules, and learning materials and establishing a standardised taxonomy for content categorization. By doing so, we aim to create a consistent and navigable learning environment that supports seamless content delivery.

#### 4.3.1.3 Assessment and Grading Criteria

Customizing Moodle will also involve defining assessment and grading criteria. This includes configuring various types of assessments, grading scales, and evaluation methods. Our goal is to tailor these criteria to match the institution's pedagogical approach and assessment standards, fostering a fair and transparent grading system.

#### 4.3.1.4 Integration with External Systems

To enhance the functionality of Moodle, we will explore the integration of external systems and tools. This could involve integrating with student information systems, authentication systems, or third-party educational applications. The defined parameters will guide the extent and nature of these integrations, ensuring compatibility and interoperability.

### 4.3.2 Constraints and Limitations

While the parametrization of Moodle offers significant flexibility, it is essential to acknowledge the constraints and limitations that may impact the customization process.

#### 4.3.2.1 Technical Constraints

Technical constraints encompass the limitations imposed by the existing technological infrastructure. This could include considerations related to server capabilities, bandwidth, and compatibility with browsers and devices. Understanding these constraints will inform decisions regarding the feasibility and scalability of certain customizations.

#### 4.3.2.2 Budgetary Limitations

Budgetary considerations play a crucial role in determining the scope of parametrization. Certain customizations may require investment in additional plugins, modules, or professional services. By identifying budgetary limitations upfront, we can prioritise customizations based on their impact and alignment with institutional goals.

#### 4.3.2.3 Time Constraints

The timeline for the parametrization project is another critical factor. Time constraints may arise from academic calendars, peak usage periods, or other time-sensitive considerations. Clearly defining these constraints will guide the project schedule and ensure realistic expectations regarding the pace of customization.

#### 4.3.2.4 Stakeholder Acceptance

The acceptance and feedback of stakeholders, including educators, students, and administrative staff, are integral to the success of parametrisation. Recognising potential resistance or challenges in stakeholder acceptance will help develop effective communication, training, and support strategies.

By establishing these defined parameters, constraints, and limitations, we create a framework for the systematic and purposeful customization of Moodle, aligning it with the institution's vision for an enhanced and tailored learning experience.

## 4.4 DCM System Architecture

### 4.4.1 Moodle Components

#### 4.4.1.1 Core Components

##### 4.4.1.1.1 Moodle Core

The core platform is at the heart of the Moodle system, providing essential functionalities such as user management, course creation, and content delivery. The core is the foundation upon which additional features and customizations are built. Parametrisation efforts will closely involve configurations within the Moodle core to align the platform with the institution's requirements.

##### 4.4.1.1.2 Database

The database is a critical component that stores user data, course content, and system configurations. Understanding the database structure is vital for parametrization, as certain customisations may involve data manipulation or the creation of new tables to support additional features.

#### 4.4.1.1.3 User Interface

The user interface components encompass the design and layout of Moodle, including themes, templates, and navigation structures. Customising the user interface is a key aspect of parametrisation, as it directly impacts the user experience. This involves configuring themes to match the institution's branding and optimising navigation for user-friendly access to features.

### 4.4.1.2 Modular Components

#### 4.4.1.2.1 Plugins and Modules

Moodle's modular architecture allows for integrating plugins and modules to extend its functionality. Plugins can include activities, blocks, authentication methods, and more. Parametrisation efforts will involve selecting, configuring, or developing plugins to enhance specific features, such as assessments, communication tools, or integrations with external systems.

#### 4.4.1.2.2 Themes

Themes dictate the visual presentation of Moodle. Customising themes is part of parametrisation, ensuring that the look and feel align with the institution's branding and preferences. This involves adjusting colour schemes, layouts, and incorporating institutional logos to create a cohesive online environment.

### 4.4.1.3 Integration Components

#### 4.4.1.3.1 External Integrations

Moodle can be integrated with external systems to enhance its capabilities. This includes integration with student information systems, authentication services, and other educational tools. Parametrisation will define the scope and configuration of these integrations to ensure seamless data flow and interoperability.

#### 4.4.1.3.2 Application Programming Interfaces

Moodle provides APIs that enable communication with external applications. Understanding and leveraging these APIs is crucial for parametrisation involving custom applications or third-party tools. This ensures that data exchange between Moodle and external systems occurs efficiently and securely.

In summary, a comprehensive understanding of Moodle's system architecture, encompassing core components, modular elements, and integration points, is essential for the successful parametrisation of the platform. This knowledge forms the basis for tailoring Moodle to meet the specific needs and objectives of the educational institution.

## 4.5 Parametrisation Strategy

Parametrising Moodle involves tailoring the platform to meet specific customisation requirements, defining user roles and permissions, and addressing data migration considerations. This section outlines the comprehensive strategy for these critical aspects of the parametrisation process.

### 4.5.1 Customisation Requirements

#### 4.5.1.1 Course Customisation

*Procedure for Teachers:*

Teachers initiate course customisation through the following steps:

1. **Course Creation:**

  - Teachers access the Moodle platform, leveraging the course creation features within the Moodle core.
  - Customisation involves setting up course details, including name, description, and enrolment methods.
2. **Content Customisation:**
    - Utilising the course content editor, teachers customise learning materials, incorporating text, multimedia, and interactive elements.
    - Activities and resources, such as quizzes, forums, and assignments, can be added, configured, and customised within the course structure.
3. **Theme Customisation:**
    - Teachers may have limited access to theme customisation based on institutional policies.
    - Customising themes involves selecting colour schemes, adding logos, and adjusting layouts for a personalised learning environment.

#### 4.5.1.2 Institutional Branding

*Procedure for Administrators:*

Administrators manage institutional branding through the following procedures:

1. **Theme Configuration:**
    - Accessing theme settings, administrators configure the overall appearance of the Moodle site.
    - This includes applying the institution's branding elements, such as logos, colour schemes, and custom CSS, for a consistent look and feel.
2. **Homepage Customisation:**
    - Administrators may customise the Moodle homepage to highlight institutional announcements, events, or featured courses.
    - Configuration involves adjusting blocks, banners, and featured content to align with the institution's communication strategy.

### 4.5.2 User Roles and Permissions

#### 4.5.2.1 Role Definition

*Procedure for Administrators:*

Administrators define user roles with the following steps:

1. **Role Creation:**
    - Define custom roles based on the institution's organisational structure and user responsibilities.
    - Create roles for teachers, students, administrative staff, and any other specific roles required.

#### 4.5.2.2 Permission Assignment

*Procedure for Administrators:*

Administrators assign roles and permissions as follows:

1. **Role Assignment:**
    - Assign users to specific roles based on their responsibilities within the institution.
    - Teachers may have additional permissions for course creation and management, while students will have access to enrolled courses.
2. **Fine-Grained Permissions:**

  - Utilise fine-grained permissions to control access to specific features and activities within courses.
  - This involves configuring permissions for activities such as grading, forum moderation, and resource creation.

### 4.5.3 Data Migration Considerations

#### 4.5.3.1 Pre-Migration Preparation

*Procedure for Data Administrators:*

Data administrators undertake pre-migration tasks:

1. **Data Audit:**
   - Conduct a thorough audit of existing data, including user profiles, course content, and activity records.
   - Identify data to be migrated, archived, or deprecated based on institutional policies.
2. **Backup Procedures:**
   - Implement robust backup procedures to ensure data integrity during migration.
   - Create backups of the Moodle database and associated files.

#### 4.5.3.2 Migration Execution

*Procedure for Data Administrators:*

Data administrators execute the migration process:

1. **Data Transfer:**
   - Utilise Moodle's built-in migration tools or third-party plugins to transfer data from the existing system to the parametrised Moodle instance.
   - Verify data integrity and address any issues that may arise during migration.
2. **User Communication:**
   - Communicate migration timelines, procedures, and potential disruptions to users.
   - Provide support channels for users encountering issues during or after migration.

This parametrisation strategy ensures a systematic and user-focused approach to customising Moodle, defining user roles, and managing data migration. Regular communication, training sessions, and ongoing support are essential components of a successful parametrisation implementation.

## 4.6 Technical Details

This section delves into the intricacies of Moodle's technical configuration, including platform settings, plugin integration, and database configuration.

### 4.6.1 Moodle Configuration Settings

#### 4.6.1.1 Site Administration

In Moodle Configuration, site administration involves various adjustments. This includes fine-tuning general settings such as the site name, description, and primary language settings to align with institutional requirements. Security settings are implemented, including SSL certificates for secure data transmission and configuring password policies and account lockout settings to enhance platform security. Performance optimisation focuses on fine-tuning caching mechanisms to optimise page load times and configuring session handling and file storage for optimal performance.

#### 4.6.1.2 Course and Activity Settings

Course and activity settings in Moodle Configuration involve configuring enrolment methods based on institutional preferences, defining course access restrictions and prerequisites. Gradebook configuration allows customisation of grading scales, grade categories, and calculation methods, along with enabling features like grade letters and outcomes based on assessment criteria. Activity modules, such as forums, quizzes, and assignments, are configured to align with pedagogical goals. Settings for interactive activities, including discussion forums and collaborative assignments, are fine-tuned.

### 4.6.2 Plugin Integration

#### 4.6.2.1 Plugin Selection

Plugin integration in Moodle Configuration involves a thorough assessment of the compatibility and reliability of third-party plugins before integration. It includes verifying plugin support for the Moodle version in use. The installation process utilises Moodle's plugin installation interface to integrate selected plugins. Configuration of plugin settings ensures proper functionality within the Moodle environment. Custom plugin development is considered for unique institutional requirements, following Moodle's development guidelines and best practices for seamless integration.

### 4.6.3 Database Configuration

#### 4.6.3.1 Database Selection

Database considerations in Moodle Configuration focus on selecting an appropriate database engine based on institutional infrastructure and performance considerations. Configuration of database connection settings is crucial for optimal performance. Table prefixing is implemented to enhance security and avoid conflicts in shared database environments. Backup and restore procedures are established for the Moodle database, including regular backups and testing of database restoration processes to ensure data integrity and system recovery.

This technical configuration lays the foundation for a stable and efficient Moodle platform. Careful consideration of security, performance, and customisability ensures a tailored and reliable learning environment.

## 4.7 User Interface Design

This section focuses on the visual aspects of the Moodle platform, emphasising theme customisation and branding elements to create an engaging and cohesive user experience.

### 4.7.1 Theme Customisation

#### 4.7.1.1 Theme Selection

In Moodle configuration, theme evaluation becomes pivotal, focusing on assessing available Moodle themes based on responsiveness, user-friendliness, and compatibility with the institution's branding. Factors such as navigation styles, colour schemes, and layout flexibility are meticulously considered during this evaluation. Administrators are then faced with the decision of opting for a pre-built theme or investing in custom development. This decision hinges on evaluating the level of customisation required and the resources available for ongoing maintenance.

#### 4.7.1.2 Theme Configuration

Upon theme selection, the configuration phase commences. Colour and styling customisation takes the forefront, involving the adjustment of the colour palette to align with the institution's branding guidelines. Font styles, sizes, and spacing are configured for readability and visual appeal. Layout and blocks are fine-tuned to optimise user navigation and content visibility, with special attention given to configuring blocks and their positioning for an intuitive and organised user interface. Responsive design is imperative to ensure the selected theme accommodates users on various devices, with extensive testing conducted across different screen sizes to guarantee a seamless experience.

### 4.7.2 Branding Elements

Moving on to branding elements, administrators delve into logo and icon customisation within the Moodle configuration.

#### 4.7.2.1 Logo and Icons

The adequate logo is uploaded and configured in Moodle configuration to ensure consistent branding. Logo dimensions are optimised to suit the theme's header, maintaining visual balance. Custom icons for activities, courses, and resources are considered to enhance visual recognition, with a keen eye on ensuring alignment with the overall design language.

#### 4.7.2.2 Messaging and Language

Messaging and language customisation further contribute to the overall branding elements within Moodle configuration. Custom login page messages are personalised to convey institution-specific information or announcements, leveraging Moodle's customisation options to enhance communication. Language strings are tailored to align with institutional terminology and preferences, with provisions for multilingual support if applicable.

The careful selection, meticulous configuration of themes, and thoughtful incorporation of branding elements collectively contribute to creating an aesthetically pleasing and user-centric Moodle interface. This approach enhances user engagement and fosters a sense of institutional identity within the e-learning environment.

## 4.8 Coping with Accessibility Issues

Since the CSP DCM is a Moodle instantiation, it uses Moodle built-in accessibility-driven strategies, mechanisms and standards to cope with accessibility issues. Moodle, as one of the world’s leading LMS, places a high priority on ensuring accessibility for all users, following the Web Content Accessibility Guidelines (WCAG) and aligning with the European Accessibility Act. Moodle’s commitment to inclusivity means that its platform offers a range of features to ensure that all learners, including those with disabilities, can engage fully with online content.

Furthermore, as an open-source platform, Moodle benefits from a global community of developers and educators who contribute regularly to its accessibility improvements. Each Moodle release incorporates feedback from users and accessibility audits to address new challenges and enhance the platform’s usability.

The following sections outline the specific mechanisms and standards used by Moodle to cope with accessibility issues. For further information, please refer to the Moodle Accessibility documentation page [44].

### 4.8.1 WCAG 2.1 Compliance and Accessibility Standards

Moodle adheres to WCAG 2.1 Level AA guidelines, which address a wide array of accessibility considerations, including screen reader compatibility, keyboard navigation, colour contrast, and adaptable text sizing. This ensures that Moodle can be accessed by users with diverse abilities and disabilities, including visual, auditory, and motor impairments.

### 4.8.2 Screen Reader Compatibility

To support visually impaired users, Moodle is designed to work smoothly with screen readers such as Job Access With Speech (JAWS), NonVisual Desktop Access (NVDA), and VoiceOver. Key Moodle components, including navigation menus, interactive elements, and text content, are structured with appropriate semantic HTML and Accessible Rich Internet Applications (ARIA) roles. These assistive technologies provide auditory feedback, allowing users to understand and navigate the platform’s structure effectively.

### 4.8.3 Keyboard Accessibility

Moodle ensures that all interactive elements, such as buttons, menus, and form fields, can be accessed and operated via keyboard. Users with mobility impairments or those unable to use a mouse can navigate Moodle’s interface through tabbing and keyboard shortcuts. Additionally, Moodle provides focus indicators to show the current element in focus, enhancing usability for keyboard-only users.

### 4.8.4 Text and Contrast Adjustments

Moodle supports high contrast themes and allows users to adjust text sizes to accommodate users with visual impairments. Through CSS and theme customisation options, instructors and administrators can enhance readability by optimising colour contrast and font settings. Moodle's core themes, like Boost, provide out-of-the-box options for clear, readable content that aligns with accessibility best practices.

### 4.8.5 Captioning and Transcripts for Multimedia

To ensure content is accessible to hearing-impaired users, Moodle encourages the use of captioning and transcripts for video and audio content. Plugins such as Poodll and resources like the ATTO editor allow instructors to include captions in multimedia files. Additionally, Moodle supports integration with third-party tools for automatic captioning, providing real-time text alternatives for spoken content.

### 4.8.6 Customisable Course Layouts and User Preferences

Moodle offers flexible course layouts and navigation structures that instructors can customise to support accessibility needs. Users can personalise settings to adjust fonts, display formats, and notification preferences, helping those with cognitive impairments or learning disabilities manage their learning environment effectively.

### 4.8.7 Accessibility Checker and Content Design Tools

The ATTO Editor in Moodle includes a built-in accessibility checker that identifies issues within course content, such as missing alt text on images or incorrect heading structures. This tool assists instructors in creating accessible materials and provides recommendations for resolving any issues it detects. By streamlining the accessibility review process, Moodle helps educators build inclusive courses without extensive technical knowledge.

### 4.8.8 Alternative Text for Images and Visual Content

Moodle encourages and enforces the use of alternative (alt) text for images, charts, and other visual elements to aid users who rely on screen readers. This feature is essential for providing context to visual information, ensuring that visually impaired learners have access to descriptive information that communicates the purpose of non-text content.

### 4.8.9 Integrations with Accessibility Plugins and Assistive Technology

Moodle’s open-source nature allows for integration with a range of accessibility-focused plugins, including those that provide enhanced screen magnification, alternative text descriptions, and text-to-speech functionality. Additionally, Moodle integrates with learning and assistive technologies commonly used in educational environments, like Braille displays and voice recognition software, to broaden access for students with varying needs.

## 4.9 Training and Documentation

This section outlines the strategies for training end-users and provides comprehensive documentation for administrators to ensure effective implementation and utilisation of the parametrised Moodle platform.

### 4.9.1 End-User Training

#### 4.9.1.1 Training Programmes

The End-User Training Strategy encompasses a series of initiatives designed to empower users with the necessary skills and knowledge for seamless interaction with the parametrised Moodle platform.

**Training Needs Assessment**: An initial assessment is conducted to identify the specific training needs of different user groups, such as students and teachers. Training programmes are then tailored to address varying levels of familiarity with the Moodle platform.

**Training Materials Development**: User-friendly training materials, including manuals, video tutorials, and interactive guides, are created. The content aligns with parametrisation changes and focuses on key features relevant to end-users.

**Training Sessions**: Live or virtual training sessions are scheduled to accommodate diverse learning preferences. These sessions provide hands-on practice opportunities to reinforce understanding.

**Feedback Mechanism**: A feedback mechanism is established to gather insights from end-users during and after training sessions. This feedback is used to improve training materials and delivery methods continuously.

#### 4.9.1.2 End-User Support

Various mechanisms are in place to offer ongoing support to end-users.

**Helpdesk and FAQs**: A dedicated helpdesk is set up to address user queries promptly. Additionally, a comprehensive Frequently Asked Questions (FAQs) section is developed to empower users with self-help resources.

**Community Forums**: Forums are created to foster a sense of community where users can share experiences and tips. Moderators are assigned to facilitate discussions and provide expert assistance.

### 4.9.2 Administrator Documentation

#### 4.9.2.1 Configuration Guides

Administrator Documentation provides administrators with the necessary information to manage and maintain the parametrised Moodle platform effectively.

**Parametrisation Documentation**: Detailed documentation on the parametrisation process is provided, including step-by-step guides for administrators. The documentation includes screenshots, code snippets, and troubleshooting tips.

**Plugin Integration Guide**: The integration of any custom or third-party plugins is documented, specifying configurations and dependencies. Potential challenges and their resolutions are highlighted.

**Data Migration Procedures**: Procedures for migrating existing data to the parametrised Moodle platform, including data backup and restoration instructions, are outlined.

**Security Best Practices**: Emphasis is placed on security best practices and configurations to safeguard user data and maintain system integrity. Guidelines on regular security audits are provided.

**System Maintenance**: Routine maintenance tasks, including system updates, backups, and performance optimisation, are documented. Periodic reviews of documentation are scheduled to ensure relevance.

Effective training and comprehensive documentation contribute significantly to successfully adopting the parametrised Moodle platform, ensuring that end-users and administrators can confidently leverage the platform's features.

## 4.10 Logistics and Processes

### 4.10.1 Introduction

Moodle, a preeminent Learning Management System (LMS), has become a linchpin in the online education ecosystem. This report explores the intricate technical facets of user authentication, login, and logout processes within a highly evolved Moodle system. This analysis aims to unravel the technical underpinnings shaping the user experience, from cryptographic protocols to session management intricacies.

### 4.10.2 User Authentication Process

The user authentication process commences with users providing credentials on the login page. The Moodle system, leveraging robust cryptographic hashing algorithms, securely stores password hashes in its user database. Upon user input, a secure hash function validates the entered password against the stored hash, ensuring password integrity without compromising user security.

Successful authentication triggers the generation of a session-specific authentication token. This token, often a JSON Web Token (JWT), encapsulates user identity and is signed with a secret key. The token becomes the cornerstone for subsequent interactions within the user session. The initiation of a user session involves the system storing the authentication token securely, often in server-side session storage or client-side cookies with proper security flags.

Access control mechanisms follow, verifying user roles and permissions against the stored information. Role-based access control (RBAC) is typically employed, allowing fine-grained control over user privileges within the Moodle system. This rigorous authentication process ensures user identity and establishes the foundation for secure and personalised learning experiences.

### 4.10.3 User Login Process

Users traverse the login process post-authentication, stepping into a dynamically enriched Moodle environment. The redirection to the user's dashboard involves server-side logic, processing user roles and permissions to tailor the dashboard content. Session management comes to the fore, with the system continuously updating session data, tracking user actions, and maintaining state information.

Activities and interactions are logged in server-side databases, providing a comprehensive audit trail. This logging mechanism serves dual purposes: refining the user experience based on historical data and meeting regulatory compliance requirements. Notifications and messages are orchestrated through real-time communication protocols, often relying on WebSockets, ensuring timely delivery and user engagement.

From a technical standpoint, the login process is not just a presentation layer transition but a synchronisation of stateful information and dynamic content generation, solidifying Moodle's reputation for a responsive and adaptive LMS.

### 4.10.4 User Logout Process

Logout, though seemingly straightforward, involves meticulous backend operations. Initiating the logout process triggers the termination of the user's session. The authentication token, often stored as an HTTP cookie, is invalidated server-side to prevent unauthorised access. Simultaneously, server-side session data is purged, ensuring the removal of any residual user-specific information.

Data cleanup extends to client-side storage, where cookies and local storage items associated with the user session are expunged. The process is often augmented with secure logout protocols, requiring re-authentication for subsequent sessions. A secure logout acknowledgement, usually an HTTP 200 OK response, is returned to the client, confirming the successful termination of the session.

From a technical lens, the logout process is not merely a disconnection event, but an orchestrated set of operations aimed at eradicating traces of user information and ensuring the integrity of the Moodle system.

### 4.10.5 Session Management and Security Measures

Central to the user experience is the nuanced realm of session management. Moodle employs a combination of server-side and client-side session storage mechanisms. Server-side sessions, often stored in databases, facilitate scalability and resilience. Concurrently, client-side cookies, fortified with Secure and HttpOnly flags, are employed for efficient state management on the user's device.

Security measures are paramount in Moodle's architecture. Sensitive data, such as authentication tokens and passwords, undergo encryption using industry-standard algorithms. Regular security audits, penetration testing, and adherence to best practices are the crux of Moodle's defensive strategy. Continuous monitoring of potential vulnerabilities and prompt application of security patches mitigate emerging threats.

The evolving threat landscape mandates an adaptive approach. Regular system updates are conducted with caution to avoid disruptions, address security vulnerabilities and ensure compatibility with emerging standards. Moodle's commitment to security transcends a mere compliance checkbox; it's a dynamic process ingrained in the system's DNA.

### 4.10.6 Continuous Improvement and Adaptation

Technical evolution is synonymous with Moodle's trajectory. Continuous improvement involves meticulous analysis of user feedback, system performance metrics, and emerging technologies. The development team, equipped with agile methodologies, iteratively refine features, enhances user interfaces, and optimises existing processes.

Innovation extends to integrating advanced features driven by emerging technologies such as machine learning and adaptive learning algorithms. The user interface undergoes iterative design cycles guided by usability studies and human-computer interaction principles. The Moodle platform is a testament to the confluence of pedagogy and technology, providing an environment that facilitates learning and adapts to the dynamic needs of educators and learners alike.

### 4.10.7 Conclusion

In conclusion, Moodle's technical intricacies of user authentication, login, and logout processes elucidate a sophisticated architecture designed for robustness and adaptability. The cryptographic underpinnings, session management strategies, and security measures collectively contribute to Moodle's reputation as a leading LMS.

As technology advances, Moodle will not be a static entity but a dynamic platform that evolves with the educational landscape. This report, a technical journey through Moodle's core processes, is a testament to its commitment to technical excellence, security, and the seamless delivery of a transformative online learning experience.

## 4.11 E-Forms

A variety of templates and e-forms have been developed to streamline the administrative processes associated with the CyberSecPro programme. As mentioned in section 3.1.6, Annex C provides evaluation templates to collect feedback on the CyberSecPro training modules from trainers and trainees. This feedback is paramount for continuously improving the CSP training programme and ensuring that it meets the needs of participants and HEIs in the future.

Additionally, a template for the CSP modules planning offer was developed and presented in the following subsection. These templates will be available in the DCM and continuously updated to meet the project needs and according to the feedback received.

### 4.11.1 Template for planning the offering of CSP Modules

In this section, we provided a template for offering CSP Modules (Table 30). The template might evolve during the project, being constantly updated in the DCM. This template applies to deliverables D3.3-D3.5.

Table 30: Template for planning the CSP Modules offering.

| CSP Module Elements | CSP Module [Fields legend] | CSP Module Information |
|---|---|---|
| **Overview** | **Code**<br>*Mandatory field. Code format:*<br>*For general modules: CSP[n]_x*<br>*[n] is the CSP module number (currently between 001 and 012)*<br>*x is the module offering type (see below)*<br>*For sector-specific modules: CSP[n]_x_y*<br>*[n] is the CSP module number (currently between 001 and 012)*<br>*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**<br>*Mandatory field. The title of the module as defined in the CSP catalogue (currently in D4.1)* | |
| | **Title of the implemented CSP module**<br>*Mandatory field. 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**<br>*Mandatory field. 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)**<br>*Mandatory field. Mapping to the 10 selected CSP knowledge areas defined in D2.3.* | |
| | **Indicate whether in the implemented CSP module, learners will learn how to implement EU cybersecurity standards, policy and regulatory principles as required to report on the respective KPI for impact/outcome**<br>*Mandatory field. Yes (also if a part of the module covered this topic) or No (otherwise)* | |
| | **Category/ies of capabilities**<br>*Mandatory field. Mapping to the 4 category/ies of capabilities defined in the CSP Grant Agreement.* | |
| | **Learning outcomes and targets** | |

| | | |
|---|---|---|
| | *Mandatory field. 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**<br>*Mandatory field. 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**<br>*Mandatory field. Indicates General, Maritime, Health, or Energy* | |
| | **Pre-requisites**<br>*Mandatory field. 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)**<br>*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**<br>*Mandatory field. 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**<br>*Programming task, essay, presentation, test-exam, mutual peer-review among students, other* | |
| | **Level**<br>*Mandatory field. B (Basic), A (Advanced)* | |
| | **Language**<br>*Mandatory field. Indicates the spoken and the languages for the material and the assessment/evaluation* | Spoken:<br>Material:<br>Assessment: |
| **Management/ Logistics** | **Provider(s)**<br>*Mandatory field. Name(s) of the providing organisation(s), e.g. beneficiary/ies* | |
| | **Contact**<br>*Mandatory field. Full name(s) of the main contact person(s) including their email address* | |
| | **Trainer(s)**<br>*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* | |

<table>
<tr><td rowspan="10"></td><td colspan="2"><b>Tool(s) to be used</b><br><i>Mandatory field. A list of tools that are to be used for the implemented CSP module.</i><br><i>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”.</i></td><td></td></tr>
<tr><td colspan="2"><b>Registration procedure</b><br><i>How (e.g. where and when registration of learner will take place) will learner have to register.</i></td><td></td></tr>
<tr><td colspan="2"><b>Admission criteria</b><br><i>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).</i></td><td></td></tr>
<tr><td colspan="2"><b>ECTS</b><br><i>The number of ECTS</i></td><td></td></tr>
<tr><td colspan="2"><b>Certificate of Attendance (CoA)</b><br><i>Mandatory field. Indicates Yes or No (and the conditions for yes, e.g. partial or full attendance, passing of exam)</i></td><td></td></tr>
<tr><td colspan="2"><b>Exact dates, when offered</b><br><i>Mandatory field. 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</i></td><td></td></tr>
<tr><td rowspan="4"><b>Schedule and duration</b><br><i>Mandatory field.</i></td><td><i>Duration of the implemented CSP module (in hours).</i></td><td rowspan="4"></td></tr>
<tr><td><i>Duration of prefabricated teaching video(s) from the CSP module that will be used in the implementation (in hours).</i></td></tr>
<tr><td><i>Estimated duration for students online-interaction during the implemented CSP module (in hours).</i></td></tr>
<tr><td><i>Frequency, duration (in hours), and rhythm of assignments if applicable.</i></td></tr>
<tr><td rowspan="4"><b>Materials</b></td><td colspan="2"><b>Location of the learning and training materials, incorporating text and multimedia, e.g. manuals, video tutorials, and interactive guides</b><br><i>Link to DCM once available, otherwise other link.</i></td><td></td></tr>
<tr><td colspan="2"><b>Location of activity modules, such as forums, quizzes, and assignments</b><br><i>Link to DCM once available, otherwise other link.</i></td><td></td></tr>
<tr><td colspan="2"><b>Location of community support</b><br><i>Link to DCM once available, otherwise other link.</i></td><td></td></tr>
<tr><td colspan="2"><b>Location of administrator documentation and configuration guides of tools used</b></td><td></td></tr>
</table>

| | | |
|---|---|---|
| | *Link to DCM once available, otherwise other link.* | |
| **Outcomes** | **Evaluation method(s)**<br>*Mandatory field. Method for the evaluation of learner performance (indicates physical and/or virtual tests, participation, exercises, etc.).* | |
| | **Evaluation and verification of learning outcomes**<br>*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)** | **Price/Fee** | |
| | **Scholarships/sponsorships**<br>*Number of offered cost free registrations*<br>*In the collection form some free text to describe the scenario, e.g. discount options and the respective conditions, is useful.* | |
| **Data Protection** | *Conditions of data collection and processing by the module provider, e.g. with respect to GDPR compliance, purpose of collection (e.g. monitoring progress or gathering feedback), processing (analytics) tools, receiver of data, duration of storage, protection tools* | |

# 5 Conclusions

This deliverable within the CyberSecPro project focuses on the structure, requirements, and specifications of the CyberSecPro education and training programme. The report outlined 12 core cybersecurity training modules, syllabi, critical sector-specific components, and a dynamic curriculum management system. The deliverable covered enrolment procedures, templates, and e-forms to facilitate training ─ emphasising consistency, quality, and relevance in cybersecurity education. Additionally, it discussed the programme's adaptability through dynamic curriculum management and provided comprehensive details of its components and procedures. Based on this deliverable, specific cybersecurity curricula for the energy, health and maritime sectors are expected to be developed and managed with the help of CyberSecPro DCM.

# References

[1] P. Rathod, P. Ofem, N. Polemi, T. Hynninen, R. G. Lugo, C. Alcaraz, K. Kioskli and K. Rannenberg, “Cybersecurity practical skills gaps in Europe: Market demand and analysis,” Deliverable D2.1, CyberSecPro-EU Digital Europe Programme Innovation Project. 2023. [Online]. Available: cybersecpro-project.eu/wp-content/uploads/2023/10/D2.1-Cybersecurity-Practical-Skills-Gaps-in-Europe-v.1.0.pdf

[2] R. Lugo, P. Rathod, P. Ofem, L. Johannesburg, N. Nikolaou, D. Siaili, K. Kasepõld, T. Sõmer, “Blended CyberSecPro Technological Training Interactive Technologies and Academic Practice,” Deliverable D2.2, CyberSecPro- EU Digital Europe Programme Innovation Project. 2023. [Online]. Available once released publicly : https://www.cybersecpro-project.eu/index.php/deliverables/

[3] A. Lieberknecht, “CyberSecPro Programme Specifications,” Deliverable D2.3, CyberSecPro- EU Digital Europe Programme Innovation Project. 2023. . [Online]. Available once released publicly : https://www.cybersecpro-project.eu/index.php/deliverables/

[4] N. Kaloudi and P. Håkon Meland, “CyberSecPro Training Operational Plan,” Deliverable D4.1, CyberSecPro-EU Digital Europe Programme Innovation Project. 2023. . [Online]. Available once released publicly : https://www.cybersecpro-project.eu/index.php/deliverables/

[5] European Union Agency for Cybersecurity, ECSF (2022), "European cybersecurity skills framework, European Union Agency for Cybersecurity," https://data.europa.eu/doi/10.2824/859537

[6] European Union Agency for Cybersecurity, Nurse, J., Adamos, K., Grammatopoulos, A. et al., Addressing the EU cybersecurity skills shortage and gap through higher education, 2021, https://data.europa.eu/doi/10.2824/033355

[7] European Cybersecurity Agency ENISA (2021), “Addressing Skills Shortage and Gap through Higher Education”, https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

[8] European Cybersecurity Agency ENISA (2020), “Cybersecurity Skills Development in the EU”, https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[9] J. L. Hall and A. Rao, "Non-Technical skills needed by cyber security graduates," 2020 IEEE Global Engineering Education Conference (EDUCON), Porto, Portugal, 2020, pp. 354-358, doi: 10.1109/EDUCON45650.2020.9125105.

[10] European Cybersecurity Agency ENISA (2022), “European Cybersecurity Skills Framework (ECSF), https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework [

[11] European Commission’s Joint Research Centre (2019), A Proposal for a European Cybersecurity Taxonomy, https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

[12] Rathod P. et al., (2021). European Cybersecurity Education and Professional Training: Minimum Reference Curriculum, European Cyber Security Organisation.

[13] Lehto, M. (2022). Development Needs in Cybersecurity Education: Final report of the project. *Informaatioteknologian tiedekunnan julkaisuja*, (96).

[14] European Cyber Security Body of Knowledge (2019): https://www.cybok.org/

[15] EU Security Union Strategy: connecting the dots in a new security ecosystem (2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

[16] Rathod, P. (2019). Towards European Cyber Security Professional Workforce Development Framework–successful practices and outcomes of the European Case, APWG EU Symposium on Electronic Crime Research (eCrime 2019 EU), Barcelona, Spain

[17] Rathod, P., Kämppi, P. (2020). Cybersecurity Workforce Capacity Building: a case of specialisation studies within the undergraduate programme. In ICCWS 2020 15th International Conference on Cyber Warfare and Security. USA, AC and publishing limited.

[18] National Institute of Standards and Technology. (2021). National Initiative for Cybersecurity Education (NICE). https://www.nist.gov/itl/applied-cybersecurity/nice

[19] Armstrong, P. (2010), Bloom’s Taxonomy. Vanderbilt University Center for Teaching, https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

[20] European e-Competence Framework, https://www.ecompetences.eu

[21] EU Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[22] Cybersecurity Education Curricula 2017 (CSEC 2017) : http://csec2017.org

[23] Cyber Education Project (CEP) : http://cybereducationproject.org/about/

[24] Anderson, L. W., & Krathwohl, D. R. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom’s taxonomy of educational objectives. New York: Longman

[25] Curricula Recommendations. Association for Computing Machinery (ACM). Retrieved from http://acm.org/education/curriculum-recommendations

[26] Cybersecurity curriculum 2017: curriculum guidelines for undergraduate degree programmes in cybersecurity. Technical report Draft version 0.5, ACM Joint Task Force on Cybersecurity Education (2017). http://www.csec2017.org/csec2017-v-0-5

[27] Lehto, M. (2018). Cyber Security Education and Research in the Finland's Universities and Universities of Applied Sciences. In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 248-267). IGI Global.

[28] National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, ver. 2.0, https://www.nist.gov/file/359261

[29] Rathod, P., Kämppi, P. (2020). Applying LEAN Principles to Improve Introductory Cybersecurity Online Subject: Findings from the Pilot Study. In SITE 2020 10th International Conference on Society for Information Technology & Teacher Education. USA, Association for the Advancement of Computing in Education (AACE).

[30] Rathod, P., Kämppi, P. (2023). The Shifting Paradigm of "Onlife Learning" in European Higher Education Institutes (HEIs): A Case of Working-Life Competence Development Best Practices, The Journal of QUADERNI DI COMUNITÀ PERSONE, EDUCAZIONE E WELFARE NELLA SOCIETÀ 5.0 – n. 3/2023 – Reinventing University. The Digital Challenge in Higher Education, pp. 91-120, ISBN:979-12-80164-71-1

[31] A. Hank, https://www.iskysoft.com/video-editing/free-open-source-video-editor.html, May 2023.

[32] Movavi, https://www.movavi.com/suite-mac/?asrc=main_menu#main, 2024

[33] Filmora, https://filmora.wondershare.net, 2024

[34] OpenShot Video Editor, https://www.openshot.org, 2024

[35] ShotCut, https://shotcut.org, 2024

[36] LightWorks, https://lwks.com, 2024

[37] Flowblade, https://jliljebl.github.io/flowblade/, 2024

[38] Blender, https://www.blender.org/features/, 2024

[39] KDEnlive, https://kdenlive.org/en/, 2024

[40] DEEPBRAIN AI, https://www.deepbrain.io/ , 2024

[41] PICTORY AI, https://www.pictory.io/ , 2024

[42] Online Learning with The World's Most Popular LMS - Moodle, https://moodle.com/, 2024

[43] Moodle.org, https://moodle.org/, 2024

[44] Moodle.org, Accessibility, https://docs.moodle.org/402/en/Accessibility, 2023

# Annex A: CSP general modules declaration

Table 31: CyberSecPro general modules.

| Module title (ref D4.1) | Unique code (ref D4.1) | Module provider(s) - collaborations | Type of module (course, seminar, summer school, etc.) |
|---|---|---|---|
| ***CSP Module**: Cybersecurity Essentials and Management* | | | |
| Information Security Management System Audit | SLC_CSP002 | SLC | C/S |
| Security Incident and Event Management | AIT_CSP004 | AIT | C/S |
| Introduction to Information Security | LAU_CSP | LAU | C |
| Cybersecurity Management | LAU_CSP | LAU | C |
| NEW "Network Security" | - | UPRC_ UMA_ LAU | C |
| NEW " Cybersecurity Essentials | - | UPRC_ UMA_ LAU | C |
| Cybersecurity | FCT_CSP006 | FCT | C |
| Information & Communication Security | GUF_CSP003 | GUF | C |
| Energy Security Fundamentals | TUC_TUBS_CSP001 | TUC, TUBS | S |
| ***CSP Module**: Human Factors and Cybersecurity* | | | |
| Cybersecurity Working Life Practices | LAU_CSP | LAU | C, W, CS-E |
| Human Factors in Cybersecurity | TRUSTILIO_CSP001 | TRUSTILIO + TalTech | S |
| ***CSP Module**: Cybersecurity Risk Management and Governance* | | | |
| Cyber Security Risk Assessment and Management | SLC_RM001 | SLC_?? | S |
| Advanced Risk Assessment | AIT_CSP001 | AIT | C/S |
| Information and Cyber Security Management | LAU_CSP | LAU | C |

| | | | |
|---|---|---|---|
| Information Security Management | LAU_CSP | LAU | C |
| Cybersecurity Maturity Models Requirements / Auditing practices | APIRO_CSP002 | APIRO | S |
| Information Security Governance | UPRC_CSP001 | UPRC ?? +APIRO | C |
| Cybersecurity threats to Maritime Administrations | C2B_CSP004 | C2B CONSULTING | W |
| Cybersecurity and Governance | FCT_CSP003 | FCT | C |
| Risk Manager | LAU_CSP | LAU | C |
| Business Continuity | LAU_CSP | LAU | C |
| ***CSP Module**: Network Security* | | | |
| System and Network Security | AIT_CSP002 | AIT | C/S |
| Internet and Infrastructure Security | LAU_CSP | LAU | C |
| Data Networks and Information Security | LAU_CSP | LAU | C |
| Network Applications | LAU_CSP | LAU | C |
| Network and Application Security | LAU_CSP | LAU | C |
| Network and Computer Systems Security | FCT_CSP001 | FCT | C |
| Mobile Business I– Technology, Markets, Platforms, and Business Models | GUF_CSP001 | GUF | C |
| ***CSP Module**: Data Protection and Privacy Technologies* | | | |
| NEW "Privacy" | - | UMA_MAG | C |
| Data Protection and Management Law | FCT_CSP004 | FCT | C |
| Cybersecurity and Data Privacy in Information Management | FCT_CSP007 | FCT | S |
| Mobile Business II– Application Design, | GUF_CSP002 | GUF | C |

| | | | |
|---|---|---|---|
| Applications, Infrastructures and Security | | | |
| ***CSP Module**: Cyber Threat Intelligence* | | | |
| Cyber Threat intelligence and vulnerability assessment | SLC_CIT003 | SLC | S |
| Cyber Security Threat Hunting | AIT_CSP003 | AIT | C/S |
| The Landscape of Hybrid Threats | LAU_CSP | LAU | C |
| System Security | LAU_CSP | LAU | C |
| Cyber Threat intelligence | PDMFC_SINTEF_CSP002 | SINTEF, PDMFC | S |
| ***CSP Module**: Cybersecurity in Emerging Technologies* | | | |
| Enterprise Security and Practitioners | LAU_CSP | LAU | C |
| CyberSecPro Portugal Summer School | UNI_FCT_CSP001 | UNI_FCT | SS |
| Anomaly Detection Techniques | UNSPMF_CSP001 | UNSPMF | S/W |
| AI and Cybersecurity | PDMFC_SINTEF_CSP001 | SINTEF, PDMFC, UNSPMF | S |
| ***CSP Module**: Critical Infrastructure Security* | | | |
| Critical Infrastructure Protection | LAU_CSP | LAU | C |
| NEW "CPS Security" | - | UMA_LAU | C |
| Network Security | UPRC_HAF_CSP001 | UPRC_HAF | c |
| CyberSecPro Cybersecurity Executive Program Seminar | UNI_FCT_CSP002 | UNI_FCT | S |
| ***CSP Module**: Software Security* | | | |
| Maritime Cyber Security Summer School - CyberHot | UPRC_trustilio_FP_TUC_CSP001 | UPRC_trustilio_FP_TUC | S |
| NEW "Software Security" | - | UMA_MAG | C |
| Software Security | FCT_CSP002 | FCT | C |
| ***CSP Module**: Penetration Testing* | | | |

| | | | |
|---|---|---|---|
| Cybersecurity Hackathon Project | LAU_CSP | LAU | C, W, CS-E |
| Advance Cybersecurity exercises | UPRC_CSP005 | UPRC | CS-E |
| AIS hacking on hands training | C2B_CSP002 | C2B CONSULTING | C |
| ***CSP Module**: Cyber Ranges and Operations* | | | |
| Maritime Cyber Security Summer School - CyberHot | UPRC_trustilio_FP_TUC_CSP001 | UPRC_trustilio_FP_TUC | S |
| NEW "Cyber Operations | - | UMA_SLC_TalTech | C |
| AIS hacking work-place training | C2B_CSP003 | C2B CONSULTING | C |
| ***CSP Module**: Digital Forensics* | | | |
| Basic Cybersecurity exercises | UPRC_CSP006 | UPRC | CS-E |
| Computer Forensics | UMA_CSP005 | UMA | C |
| Information Security and Computer Forensics | UMA_CSP008 | UMA | C |
| Cybercrime | FCT_CSP005 | FCT | O |

Table 32: CyberSecPro health modules declaration.

| **Module title (ref D4.1)** | **Unique code (ref D4.1)** | **Module provider(s) - collaborations** | **Type of module (course, seminar, summer school, etc.)** |
|---|---|---|---|
| ***CSP Module**: Cybersecurity Essentials* | | | |
| | | | |
| ***CSP Module**: Human Factors and Cybersecurity* | | | |
| Cybersecurity and Health | trustilio_CSP003 | trusitlio + SLC | Seminar |
| ***CSP Module**: Management and Governance* | | | |
| NEW seminar UPRC attack path | - | UPRC | S |
| NEW ISO 27799 - Information security | - | APIRO | S |

| | | | |
|---|---|---|---|
| management in health using ISO/IEC 27002 | | | |
| Security of Maritime, Health & Energy Critical Information Infrastructures | UMA_UPRC_CSP001 | UMA_UPRC | S |
| ***CSP Module**: Network Security* | | | |
| Security information and event management - Endpoint protection | ITML_CSP002 | ITML | Seminar/ other-demonstration |
| ***CSP Module**: Protection and Privacy Technologies* | | | |
| | | | |
| ***CSP Module**: Threat Intelligence* | | | |
| | | | |
| ***CSP Module**: Security in Emerging Technologies* | | | |
| NEW seminar UPRC (not included in 4.1) | - | UPRC | S |
| NEW Health Anomaly Detection Seminar UNSPMF (not included in 4.1) | - | UNSPMF | S |
| ***CSP Module**: Critical Infrastructure Security* | | | |
| | | | |
| ***CSP Module**: Software Security* | | | |
| | | | |
| ***CSP Module**: Penetration Testing* | | | |
| | | | |
| ***CSP Module**: Cyber Ranges and Operations* | | | |
| Security information and event management - Alerting & Reporting | ITML_CSP001 | ITML | Seminar/ other-demonstration |
| Security information and event management - Monitoring | ITML_CSP004 | ITML | Seminar/ other-demonstration |
| ***CSP Module**: Digital Forensics* | | | |
| Security information and event management - Forensics | ITML_CSP003 | ITML | Seminar/ other-demonstration |

Table 33: CyberSecPro energy modules declaration.

| Module title (ref D4.1) | Unique code (ref D4.1) | Module provider(s) - collaborations | Type of module (course, seminar, summer school, etc.) |
|---|---|---|---|
| ***CSP Module**: Cybersecurity Essentials* | | | |
| Introduction to Cybersecurity in the Electrical Energy System | FCT_CSP008 | FCT | C |
| ***CSP Module**: Human Factors and Cybersecurity* | | | |
| NEW ISO/IEC 27019 - Information security controls for the energy utility industry | | APIRO | S |
| Security of Maritime, Health & Energy Critical Information Infrastructures | UMA_UPRC_CSP001 | UMA_UPRC | s |
| SATRA for energy | CNR_UMA_CSP001 | CNR_UMA | O |
| NEW Cybersecurity Essentials for the energy sector | | UPRC_ UMA_ LAU | C |
| ***CSP Module**: Network Security* | | | |
| | | | |
| ***CSP Module**: Data Protection and Privacy Technologies* | | | |
| | | | |
| ***CSP Module**: Threat Intelligence* | | | |
| Attacks/countermeasures/ mitigations/privacy on energy control systems (SCADA) | C2B_CSP005 | C2B CONSULTING | C |
| Cybersecurity Challenges of Electrical Energy Substations | FCT_CSP009 | FCT | C |
| ***CSP Module**: Security on Emerging Technologies* | | | |
| | | | |
| ***CSP Module**: Critical Infrastructure Security* | | | |

| | | | |
|---|---|---|---|
| Next Generation Energy Systems Security | AIT_CSP005 | AIT | C/S |
| Industrial Control Systems Security | AIT_CSP006 | AIT | C/S |
| Security in charging stations and their control systems | UMA_UCY_CSP001 | UMA_UCY | S |
| ***CSP Module**: Software Security* | | | |
| | | | |
| ***CSP Module**: Penetration Testing* | | | |
| | | | |
| ***CSP Module**: Cyber Ranges and Operations* | | | |
| | | | |
| ***CSP Module**: Digital Forensics* | | | |
| | | | |

Table 34: CyberSecPro maritime modules declaration.

| Module title (ref D4.1) | Unique code (ref D4.1) | Module provider(s) - collaborations | Type of module (course, seminar, summer school, etc.) |
|---|---|---|---|
| ***CSP Module**: Cybersecurity Essentials and Management* | | | |
| Cybersecurity Essentials | Telematics for Shipping and Transport | new | trustilio |
| ***CSP Module**: Human Factors and Cybersecurity* | | | |
| Human Centric and Secure Maritime Ecosystems | trustilio_CSP002 | trustilio + TALTECH | Seminar |
| Human Factors in maritime | new | TALTECH + trustilio | Summer School |
| ***CSP Module**: Cybersecurity Risk Management and Governance* | | | |
| Maritime Cybersecurity Risk | C2B_CSP001 | C2B CONSULTING | C |
| Security of Maritime, Health & Energy Critical Information Infrastructures | UMA_UPRC_CSP001 | UMA_UPRC | S |
| ***CSP Module**: Network Security* | | | |

| | | | |
|---|---|---|---|
| NEW Maritime Cyber pen Testing | UPRC_trustilio_FP_TUC_CSP001 | UPRC_trustilio_FP_TUC | S |
| ***CSP Module***: *Protection and Privacy Technologies* | | | |
| | | | |
| ***CSP Module***: *Threat Intelligence* | | | |
| | | | |
| ***CSP Module***: *Cybersecurity in Emerging Technologies* | | | |
| | | | |
| ***CSP Module***: *Critical Infrastructure Security* | | | |
| | | | |
| ***CSP Module***: *Software Security* | | | |
| NEW Maritime Cyber software security | UPRC_trustilio_FP_TUC_CSP001 | UPRC_trustilio_FP_TUC | S |
| ***CSP Module***: *Penetration Testing* | | | |
| AIS hacking on hands training | C2B_CSP002 | C2B CONSULTING | C |
| ***CSP Module***: *Cyber Ranges and Operations* | | | |
| AIS hacking work-place training | C2B_CSP003 | C2B CONSULTING | C |
| NEW Maritime Cyber blue team | UPRC_trustilio_FP_TUC_CSP001 | UPRC_trustilio_FP_TUC | S |
| ***CSP Module***: *Digital Forensics* | | | |
| Cybersecurity threats to Maritime Administrations | C2B_CSP004 | C2B CONSULTING | W |

# Annex B: Training offers in the 12 CSP modules

Table 35: Categorisation of training offers in the 12 CSP modules: General.

| No. | Title of CSP module | Collaboration as reported in D3.1 | Collaboration as reported in General excel | Unique code |
|---|---|---|---|---|
| *Operating the training modules on Cybersecurity Principles and Management*<br>*Operating the training modules on Cybersecurity Tools* | | | | |
| 1 | Cybersecurity Essentials and Management | LAU, UPRC, UMA, TUC, TUBS | SLC, AIT, LAU, UPRC,UMA,FCT,GUF, TUC, TUBS | CSP001_C<br>CSP001_CS-E<br>CSP001_S |
| 2 | Human Factors and Cybersecurity | TalTech, trustilio, TUBS, LAU | LAU,trustilio,TALTECH | CSP002_CS-E<br>CSP002_S<br>CSP002_C |
| 3 | Cybersecurity Risk Management and Governance | UPRC, SLC, APIRO, TUBS | SLC, AIT, LAU, APIRO, UPRC, C2B, FCT | CSP003_W<br>CSP003_S<br>CSP003_C |
| 4 | Network Security | UMA, UCY, GUF, AIT, TUBS, ITML | AIT, LAU, FCT, GUF | CSP004_S<br>CSP004_C<br>CSP004_W |
| 5 | Data Protection and Privacy Technologies | ZEL, GUF, FCT, TUBS | FCT, GUF, UMA, MAG, UCY | CSP005_CS-E<br>CSP005_S<br>CSP005_C |
| *Operating the training modules on Emerging Technologies*<br>*Operating the training modules on Cybersecurity Offensive Practices* | | | | |
| 6 | Cyber Threat Intelligence | UPRC, AIT, SLC_CIT | SLC, AIT, LAU, SINTEF, PDMFC | CSP006_S<br>CSP006_C<br>CSP006_CS-E |
| 7 | Cybersecurity in Emerging Technologies | LAU, UNSPMF, UNINOVA, FCT | LAU, FCT, UNSPMF, PDMFC, SINTEF | CSP007_C<br>CSP007_W<br>CSP007_S |
| 8 | Critical Infrastructure Security | UNINOVA, UPRC/HAF | LAU, UMA, UPRC, HAF, FCT | CSP008_W<br>CSP008_C<br>CSP008_S |

| | | | | |
|---|---|---|---|---|
| 9 | Software Security | PDMFC, FCT, TUC | UPRC, trustilio, FP, TUC, FCT, UMA, MAG, UCY | CSP009_W<br>CSP009_S<br>CSP009_C |
| 10 | Penetration Testing | FCT, C2B, LAU | LAU, UPRC, C2B | CSP010_W<br>CSP010_C<br>CSP010_S |
| 11 | Cyber Ranges and Operations | UPRC, CNR, C2B, TUC, ITML | UPRC, trustilio, FP, TUC, UMA, SLC, TalTech, C2B | CSP011_S<br>CSP011_C<br>CSP011_CS-E |
| 12 | Digital Forensics | UNINOVA, ITML, FCT | UPRC, FCT, UMA, MAG | CSP012_CS-E<br>CSP012_S<br>CSP012_C |

Table 36: Categorisation of training offers in the 12 CSP modules: Maritime.

| No. | Title of CSP module | Collaboration as reported in D3.1 | Collaboration as reported in General excel | Additional partners according to maritime | Unique code |
|---|---|---|---|---|---|
| 1 | Cybersecurity Essentials and Management | LAU, UPRC, UMA,TUC, TUBS | UPRC, LAU, SGI, TUC | trustilio | CSP001_C_M<br>CSP001_CS-E_M<br>CSP001_S_M |
| 2 | Human Factors and Cybersecurity | TalTech, trustilio, TUBS, LAU | trustilio, TalTech | | CSP002_S_M<br>CSP002_SS_M |
| 3 | Cybersecurity Risk Management and Governance | UPRC, SLC, APIRO, TUBS | UPRC, AIT, SLC | UMA | CSP003_S_M<br>CSP003_C_M |
| 4 | Network Security | UMA, UCY, GUF, AIT, TUBS, ITML | UCY, AIT | trustilio | CSP004_S_M<br>CSP004_C_M |
| 5 | Data Protection and Privacy Technologies | ZEL, GUF, FCT, TUBS | MAG, SLC, MAG | | CSP005_S_M |
| 6 | Cyber Threat Intelligence | UPRC, AIT, SLC_CIT | SLC, UPRC, AIT | | CSP006_S_M |

| | | | | | |
|---|---|---|---|---|---|
| 7 | Cybersecurity in Emerging Technologies | LAU, UNSPMF, UNI, FCT | ACEEU, SINTEF, PDMFC, UNSPMP | | CSP007_W_M<br>CSP007_S_M |
| 8 | Critical Infrastructure Security | UNINOVA, UPRC/HAF | C2B, TalTech | | CSP008_C_M<br>CSP008_S_M |
| 9 | Software Security | PDMFC, FCT, TUC | FP, MAG, TUC | | CSP009_S_M |
| 10 | Penetration Testing | FCT, C2B, LAU | FP, C2B, FP | | CSP010_W_M<br>CSP010_S_M |
| 11 | Cyber Ranges and Operations | UPRC, CNR, C2B, TUC, ITML | UPRC, trustilio, FP, TUC | | CSP011_S_M<br>CSP011_C_M |
| 12 | Digital Forensics | UNINOVA, ITML, FCT | C2B | trustilio, FP, TUC | CSP012_S_M |

Table 37: Categorisation of training offers in the 12 CSP modules: Health.

| No. | Title of CSP module | Collaboration as reported in D3.1 | Collaboration as reported in General excel | Additional partners according to health | Unique code |
|---|---|---|---|---|---|
| 1 | Cybersecurity Essentials and Management | LAU, UPRC, UMA,TUC, TUBS | UPRC, LAU, SGI | | CSP001_C_H<br>CSP001_CS-E_H |
| 2 | Human Factors and Cybersecurity | TalTech, trustilio, TUBS, LAU | trustilio, SLC, TalTech, LAU | SLC | CSP002_S_H |
| 3 | Cybersecurity Risk Management and Governance | UPRC, SLC, APIRO, TUBS | APIRO, UPRC | UMA | CSP003_S_H |
| 4 | Network Security | UMA, UCY, GUF, AIT, TUBS, ITML | Itml, TUBS | | CSP004_S_H<br>CSP004_C_H |
| 5 | Data Protection and Privacy Technologies | ZEL, GUF, FCT, TUBS | ZEL, CNR | | CSP005_W_H<br>CSP005_S_H |

| | | | | | |
|---|---|---|---|---|---|
| 6 | Cyber Threat Intelligence | UPRC, AIT, SLC_CIT | SINTEF, PDMFC, UPRC | | CSP006_S_H |
| 7 | Cybersecurity in Emerging Technologies | LAU, UNSPMF, UNINOVA, FCT | CNR, UNSPMF | | CSP007_S_H |
| 8 | Critical Infrastructure Security | UNINOVA, UPRC/HAF | AIT, UPRC, SLC, UNINOVA, PDMFC, ITML | | CSP008_S_H<br>CSP008_C_H |
| 9 | Software Security | PDMFC, FCT, TUC | FP, FCT, PDMFC | | CSP009_W_H<br>CSP009_S_H |
| 10 | Penetration Testing | FCT, C2B, LAU | LAU, TalTech, trustulio, FP | | CSP010_C_H<br>CSP010_W_H |
| 11 | Cyber Ranges and Operations | UPRC, CNR, C2B, TUC, ITML | ITML, FP, IMT | | CSP011_S_H<br>CSP011_W_H<br>CSP011_CS-E_H |
| 12 | Digital Forensics | UNINOVA, ITML, FCT | ITML, PDMFC, ZEL | | CSP012_S_H |

Table 38: Categorisation of training offers in the 12 CSP modules: Energy.

| No. | Title of CSP module | Collaboration as reported in D3.1 | Collaboration as reported in General excel | Additional partners according to energy | Unique code |
|---|---|---|---|---|---|
| 1 | Cybersecurity Essentials and Management | LAU, UPRC, UMA, TUC, TUBS | LAU, UMA, SGI, PDMFC, trustilio, TalTech, TUC, TUBS | | CSP001_C_E<br>CSP001_CS-E_E<br>CSP001_S_E |
| 2 | Human Factors and Cybersecurity | TalTech, trustilio, TUBS, LAU | SEA, LAU, TalTech, TRUST | | CSP002_CS_E<br>CSP002_S_E<br>CSP002_SS_E<br>CSP002_CS-E_E |
| 3 | Cybersecurity Risk Management and Governance | UPRC, SLC, APIRO, TUBS | UMA, CNR, SLC, APIRO | UMA, CNR | CSP003_S_E<br>CSP003_C_E |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Network Security | UMA, UCY, GUF, AIT, TUBS, ITML | UMA, AIT, TUBS | | CSP004_S_E<br>CSP004_C_E |
| 5 | Data Protection and Privacy Technologies | ZEL, GUF, FCT, TUBS | TUBS, CNR, FCT | | CSP005_S_E<br>CSP005_C_E |
| 6 | Cyber Threat Intelligence | UPRC, AIT, SLC_CIT | AIT, FCT | C2B,FCT | CSP006_S_E<br>CSP006_C_E |
| 7 | Cybersecurity in Emerging Technologies | LAU, UNSPMF, UNINOVA, FCT | UNINOVA, LAU, FCT | | CSP007_C_E<br>CSP007_S_E |
| 8 | Critical Infrastructure Security | UNINOVA, UPRC/HAF | UNINOVA, FCT, PDMFC, UMA, UCY | AIT,UCY | CSP008_C_E<br>CSP008_S_E |
| 9 | Software Security | PDMFC, FCT, TUC | UCY, FCT | | CSP009_S_E |
| 10 | Penetration Testing | FCT, C2B, LAU | UPRC | | CSP010_S_E |
| 11 | Cyber Ranges and Operations | UPRC, CNR, C2B, TUC, ITML | CNR, C2B, ITML | | CSP011_S_E<br>CSP011_C_E |
| 12 | Digital Forensics | UNINOVA, ITML, FCT | UNINOVA, FCT, PDMFC | | CSP012_S_E |

# Annex C: CyberSecPro Training Module Evaluation Template: Training Participant

Training Module Code: ________________________________

Training Module Name: ________________________________ Date: __________________

Training Module Offered by: ____________________________________________________________

Module Evaluation Feedback by Training Participant

**1. How well did you achieve this learning objective in this module?**

| | 1 To no extent | 2 To little extent | 3 To some extent | 4 To a large extent | 5 To a very large extent |
|---|---|---|---|---|---|
| Learning Objective 1 | | | | | |
| Learning Objective 2 | | | | | |
| Learning Objective 3 | | | | | |
| Learning Objective 4 | | | | | |

Note: (Learning Objectives) will be defined by the trainers based on the module syllabus.

**2. How useful to you was this module element?**

| | 1 To no extent | 2 To little extent | 3 To some extent | 4 To a large extent | 5 To a very large extent |
|---|---|---|---|---|---|
| Learning Element 1 | | | | | |
| Learning Element 2 | | | | | |
| Learning Element 3 | | | | | |
| Learning Element 4 | | | | | |

Note: (Learning Element) will be defined by the trainers based on the module syllabus. Examples of learning elements to evaluate can be lectures, group project, exercises etc.

**3. How much did you learn from this module?**

| | | | | |
|---|---|---|---|---|
| 1 To no extent | 2 To little extent | 3 To some extent | 4 To a large extent | 5 To a very large extent |

**4. Overall, how would you describe the quality of the instruction in this module?**

| | | | | |
|---|---|---|---|---|
| 1 Very poor | 2 Poor | 3 Fair | 4 Good | 5 Excellent |

**5. What skills or knowledge did you learn or improve?**

______________________________________________________________________

______________________________________________________________________

**6. How many hours per week on average did you spend on this module?**

[Drop-down options may make the evaluation easier e.g., 5 to 10, 11 to 20, 20 to 30. This will be assessed, when the from will be put online]

______________________________________________________________________

______________________________________________________________________

**7. How organised was this module?**

| | | | | |
|---|---|---|---|---|
| 1 Not organised at all | 2 Slightly organised | 3 Moderately organised | 4 Very organised | 5 Extremely organised |

**8. Would you like to recommend this module to your friends or colleagues?**

[Drop-down options may make the evaluation easier e.g., YES/NO/MAYBE/NOT SURE. This will be assessed, when the from will be put online]

______________________________________________________________________

______________________________________________________________________

**9. What would you like to say about this module to a trainee who is considering taking it in the future? For example, recommendation for the training and benefits**

______________________________________________________________________

______________________________________________________________________

**10. Would you like to provide any other comments about this module?**

______________________________________________________________________

______________________________________________________________________

# Annex D: CyberSecPro Training Module Evaluation Template: Trainer

Training Module Code: ______________________________

Training Module Name: ______________________________ Date: __________________

Training Module Offered by: _______________________________________________________

Training Provider (Trainers) Reflection Report:

**FIRST IMPRESSIONS**

**1. What do you think worked particularly well in this training module?**

__________________________________________________________________________

__________________________________________________________________________

**CONTENT**

**2. How well do you think your trainees learned:**

| | 1 Not at all | 2 A little | 3 Some | 4 Much | 5 Very much |
|---|---|---|---|---|---|
| Learning Objective 1 | | | | | |
| Learning Objective 2 | | | | | |
| Learning Objective 3 | | | | | |
| Learning Objective 4 | | | | | |

Note: (Learning Objectives) will be defined by the trainers based on the module syllabus.

**3. Is it your impression that the trainees had sufficient support to learn the topics in this module? Do you have any ideas of how to improve this?**

__________________________________________________________________________

__________________________________________________________________________

**4. Learning any topic also gives trainees the chance to learn 'transferable skills' such as writing, oral presentation, experimental design, etc. Do you think this module particularly helped your trainees improve in any of these?**

__________________________________________________________________________

__________________________________________________________________________

**TRAINEES' EFFORT AND PREPAREDNESS**

**5. Do you think your trainees put in sufficient time and effort in this module to succeed?**

| | 1 Few trainees | 2 Some trainees | 3 About half of them | 4 Many trainees | 5 Most trainees |
|---|---|---|---|---|---|
| Sufficient effort | | | | | |
| Sufficient time | | | | | |

**6. Do you have the impression the trainees had sufficient knowledge from previous modules to succeed in this module? (Yes/No)**

Do you think the trainees saw the relevance of past knowledge/modules for your subject? (Yes/No) How do you think we could improve the trainees’ preparedness?

## TEACHING

**7. Was it your impression that these tools/teaching methods worked well to support your students learning?**

| | Not relevant | 1 Not at all | 2 A little | 3 Some | 4 Much | 5 Very much |
|---|---|---|---|---|---|---|
| Lectures | | | | | | |
| Labs | | | | | | |
| Literature | | | | | | |
| Trainee activities | | | | | | |
| Seminars | | | | | | |
| Real life examples | | | | | | |
| Exercise sessions | | | | | | |
| Case studies (sector-specific) | | | | | | |
| Project work | | | | | | |
| Tools | | | | | | |
| Other: …………….. | | | | | | |

**8. Are you satisfied with how the different parts (moments) of the module were distributed? (for example, should there have been more lab or lecture?) (Yes/No) If no, how would you change this next time?**

______________________________________________________________

______________________________________________________________

**9. Do you think the trainees had a chance to practice what they were learning and received sufficient feedback during the training module?**

Do you have any suggestions that could improve this?

______________________________________________________________

______________________________________________________________

**10. Did the examination (all aspects) correspond well with the learning objectives?**

______________________________________________________________

Would you consider other ways of examination perhaps in the future (e.g. computer-assisted, quizzes, oral, group exams, written papers)?

______________________________________________________________

______________________________________________________________

**<u>ORGANISATION</u>**

**11. Was it your impression that trainees found it easy to find information about the course (e.g. schedule, literature lists, etc.)? Would you change anything to improve this?**

______________________________________________________________

______________________________________________________________

**<u>OVERALL IMPRESSION</u>**

**12. What challenges or problems did you face in this training module (if any)?**

______________________________________________________________

______________________________________________________________

**13. What would you change in this training module next time it runs? And why?**

______________________________________________________________

______________________________________________________________

**14. What kinds of teaching methods do you use in your module?**

______________________________________________________________

______________________________________________________________

Would you like to use any new teaching methods in the future? Yes/No
What kind of support would you like to make this easy?

______________________________________________________________

______________________________________________________________

### 15. Other reflections?

______________________________________________________________________________

_________________________________________________________________

**DEMOGRAPHICS**

*Total number of persons:*

*Nationalities: List ALL.*

*Level of education [undergraduate student (e.g. 10% or number of persons), BSc, postgraduate student, MSc, PhD student, PhD*

*Group ages [18-29 (e.g. 10% or number of persons), 30-39, 40-49, 50-59, 60-…]*

*Gender groups [% Male, % Female]*

# Annex E: CyberSecPro Training Module Verification Template - Preparedness Checklist (a completion guideline for D3.3-D3.5)

Training Module Code: ________________________________

Training Module Name: ________________________________

Planned date for Operation: __________________

Training Module to be Offered by: ________________________________________________________

Preparedness Checklist (Before Operation) by Trainer

## KNOWLEDGE AREA

**1. Check that the topics implemented for the module cover the preestablished "Knowledge Area(s)".**

| | KA 1 | KA 2 | KA 3 | KA 4 | … |
|---|---|---|---|---|---|
| Topic 1<br>(of the syllabus) | □ | □ | □ | □ | □ |
| Topic 2<br>(of the syllabus) | □ | □ | □ | □ | □ |
| Topic 3<br>(of the syllabus) | □ | □ | □ | □ | □ |
| Topic 4<br>(of the syllabus) | □ | □ | □ | □ | □ |

Note: The trainers will define (Topics) based on the module syllabus.

## LEARNING OBJECTIVE/OUTCOME

**2. Check that all learning objectives/outcomes are addressed by the topics/contents set out for the module.**

| | Learning Objective 1 | Learning Objective 2 | Learning Objective 3 | Learning Objective 4 | … |
|---|---|---|---|---|---|
| Topic 1<br>(of the syllabus) | □ | □ | □ | □ | □ |

| | | | | | |
|---|---|---|---|---|---|
| Topic 2 (of the syllabus) | □ | □ | □ | □ | □ |
| Topic 3 (of the syllabus) | □ | □ | □ | □ | □ |
| Topic 4 (of the syllabus) | □ | □ | □ | □ | □ |

Note: (Topics and Learning Objectives) will be defined by the trainers based on the module syllabus.

3. **Check that all learning objectives/outcomes are addressed by the practical activities established for each sector (D3.3-D3.5), marking which cover the learning activities.**

| | Learning Objective 1 | Learning Objective 2 | Learning Objective 3 | Learning Objective 4 | … |
|---|---|---|---|---|---|
| Final project | □ | □ | □ | □ | □ |
| Use case analysis | □ | □ | □ | □ | □ |
| Activity 3 | □ | □ | □ | □ | □ |
| … | □ | □ | □ | □ | □ |

Note: (Learning Objectives) will be defined by the trainers based on the module syllabus.

4. **Check that all learning objectives/outcomes are addressed by the pedagogical methods identified for the module and adapted to the design of the activities established in D3.3-D3.5.**

| | Learning Objective 1 | Learning Objective 2 | Learning Objective 3 | Learning Objective 4 | … |
|---|---|---|---|---|---|
| Flipped-Classroom | □ | □ | □ | □ | □ |
| Gamification | □ | □ | □ | □ | □ |
| Pedagogical method 3 | □ | □ | □ | □ | □ |
| Pedagogical method 4 | □ | □ | □ | □ | □ |

Note: (Pedagogical methods and Learning Objectives) will be defined by the trainers based on the module syllabus.

**SKILLS**

5. **Check that the pedagogical methods correctly address preestablished soft skills according to the definition established in D3.1.**

| | Lectures (online synchrony, face-to-face) | Asynchronous Lectures (MOOC) | Flipped-Classroom | Gamification | … |
|---|---|---|---|---|---|
| Soft Skill 1 | □ | □ | □ | □ | □ |
| Soft Skill 2 | □ | □ | □ | □ | □ |
| Soft Skill 3 | □ | □ | □ | □ | □ |
| …. | □ | □ | □ | □ | □ |

Note: (Pedagogical methods and Skills) will be defined by the trainers based on the module syllabus.

6. **Check for each of the practical activities/exercises set for D3.3-D3.5 to determine whether they fit the degree of difficulty (advanced/basic) stated for your corresponding module:**

| | Advanced | Basic |
|---|---|---|
| Activity 1<br>(of the syllabus) | □ | □ |
| Activity 2<br>(of the syllabus) | □ | □ |
| Activity 3<br>(of the syllabus) | □ | □ |
| …. | □ | □ |

**COMPLETENESS OF LEARNING ARTEFACTS**

7. **Check whether the following learning artefacts are correctly addressed and available (from the DCM platform) before the operation phase, further verifying that they follow the preestablished CyberSecPro templates:**

| | Not addressed | Requires improvement for compliance | Addressed according to the templates |
|---|---|---|---|
| Video Teaser | □ | □ | □ |
| Presentation PPT | □ | □ | □ |
| Evaluation templates (trainers/trainees) | □ | □ | □ |
| … | □ | □ | □ |

8. **Check whether all the material is available before operation and from the DCM platform – if it is possible:**

| | Not addressed | Addressed and available |
|---|---|---|
| Video Teaser | □ | □ |
| Presentation of the module | □ | □ |
| Evaluation templates for trainers | □ | □ |
| Evaluation templates for trainees | □ | □ |
| Knowledge tests | □ | □ |
| Practical activities | □ | □ |
| Additional resources (forums, chats, etc.) | □ | □ |

9. **Indicate the type of practical artefacts that will be applied for the practicalities during the operation phase:**

| | |
|---|---|
| Tools | □ |
| Real-life scenarios | □ |
| Simulators | □ |
| Emulators… | □ |
| … | □ |

**10. If the module uses tools/simulators/emulators, check whether all of these practical artefacts are available/accessible from the DCM platform, from another platform provided by the consortium, or from external entities. Likewise, check if they are ready for their final application before operation:**

| | Open source | Commercial | Available/ accessible (100%) | Available/ accessible (partially) | Ready for final application |
|---|---|---|---|---|---|
| Tool 1 | □ | □ | □ | □ | □ |
| Tool 2 | □ | □ | □ | □ | □ |
| Tool 3 | □ | □ | □ | □ | □ |
| … | □ | □ | □ | □ | □ |

**If the tool is commercial, indicate whether you have the conditions or permission to use it during the operation phase:**

________________________________________________________

________________________________________________________

**If the tool is partially available, indicate the reasons and the solutions to be adopted during the operation period:**

________________________________________________________

________________________________________________________

**11. Check for each of the activities/practical exercises set out for D3.3-D3.5 to see whether there is an associated tool:**

| | Tool 1 | Tool 2 | Tool 3 | Tool 4 | … |
|---|---|---|---|---|---|
| Activity 1 (of the syllabus) | □ | □ | □ | □ | □ |
| Activity 2 (of the syllabus) | □ | □ | □ | □ | □ |
| Activity 3 (of the syllabus) | □ | □ | □ | □ | □ |
| …. | □ | □ | □ | □ | □ |

**If there are activities without association to a tool, indicate the reasons:**

**If the tool is partially available, indicate the reasons and the solutions to be adopted during the operation period:**

# Annex F: Existing program/courses which have been reviewed/complemented/enhanced during WP3

Table 39. Existing program/courses which have been reviewed/complemented/enhanced during WP3 (Maritime sector).

| CSP Module name | Who | Academic course name | Academic program name (BSc/MSc) | University | ECTS |
|---|---|---|---|---|---|
| **CSP001_C_M: Cybersecurity Essentials and Management for Maritime** | UPRC, LAU | Information Security Management | Business Information Technology - Cybersecurity (BSc) | Laurea University of Applied Sciences | 5 |
| | | Cybersecurity management | Business Information Technology - Cybersecurity (BSc) | | 5 |
| | | Introduction to Information Security | Business Information Technology - Cybersecurity (BSc) | | 5 |
| | | Information and Cyber Security Management | Business Information Technology - Cybersecurity (BSc) | | 10 |
| | | Maritime Information Systems | Informatics (BSc) | University of Piraeus | 4 |
| | | Maritime Informatics | Informatics (MSc) | | 3 |
| **CSP003_S_M: Cybersecurity Risk Management and Governance for Maritime** | UPRC, AIT | Maritime Information Systems | Informatics (BSc) | University of Piraeus | 4 |
| | | Maritime Informatics | Informatics (BSc) | | 3 |
| | | Information Systems Security | Informatics (BSc) | | 4 |
| | | Information Systems Security Management | Cybersecurity and Data Science (MSc) | | 4 |

| CSP Module name | Who | Academic course name | Academic program name (BSc/MSc) | University | ECTS |
|---|---|---|---|---|---|
| **CSP006_SA_M: Cyber Threat Intelligence for Maritime** | UPRC, AIT | Maritime Information Systems | Informatics (BSc) | University of Piraeus | 4 |
| | | Systems Security Management | Informatics (BSc) | | 3 |
| | | Information Systems Security | Informatics (MSc) | | 4 |
| | | Maritime Informatics | Informatics (MSc) | | 3 |
| | | Information Systems Security Management | Informatics (BSc) | | 4 |
| **CSP008_C_M: Critical Infrastructure Security for Maritime** | C2B | Information Security Management | Master 2 – M2 : Gestion de la production logistique, Management Maritime et portuaire  (MSc) | Université de la cote d’Opale | 5 |
| | | Cybersecurity management | | | 2 |
| | | Introduction to Information Security | | | 5 |
| | | Information and Cyber Security Management | | | 2 |
| **CSP0011_W_M: Cyber Ranges and Operations for Maritime** | UPRC, trustilio, FP, TUC | Maritime Information Systems | Informatics (BSc) | University of Piraeus | 4 |
| | | Systems Security Management | Informatics (BSc) | | 3 |
| | | Information Systems Security | Informatics (BSc) | | 4 |
| | | Maritime Informatics | Informatics (MSc) | | 3 |
| | | Information Systems Security Management | Cybersecurity and Data Science (MSc) | | 4 |

Annex F: Existing program/courses which have been reviewed/complemented/enhanced during WP3

| CSP Module name | Who | Academic course name | Academic program name (BSc/MSc) | University | ECTS |
|---|---|---|---|---|---|
| **CSP010_W_M: Cyber Range Pen Testing Maritime** | C2B | Information and Cyber Security Management | Master 2 – M2 : Gestion de la production logistique, Management Maritime et portuaire (MSc) | Université de la cote d'Opale | 2 |
| | | Network and application security | | | 5 |
| | | Introduction to Information Security | | | 2 |
| | | Cybersecurity Working Life Practices | | | 10 |
| **CSP012_S_M: Digital Forensic for Maritime** | C2B | Cybersecurity Analyst | Master 2 – M2 : Gestion de la production logistique, Management Maritime et portuaire (MSc) | Université de la cote d'Opale | 10 |
| | | Cybersecurity management | | | 5 |
| | | Introduction to Information Security | | | 5 |
| | | Information and Cyber Security Management | | | 2 |
| **CSP002_SS_M: Human Factors of Maritime Cybersecurity** | TalTech, trustilio, Laurea | Human Factors of Maritime Cybersecurity | Masters in Cybersecurity (MSc) | Tallinn University of Technology | 2 |

Table 40. Existing program/courses  which have been reviewed/complemented/enhanced during WP3 (Health sector).

| CSP Module name | Who | Academic course name | Academic program name (BSc/MSc) | University | ECTS |
|---|---|---|---|---|---|
| **CSP008_C_H: Advanced Infrastructure Security** | UNINOVA, PDMFC | Network and Computer Systems Security | Computer Science and Engineering (MSc) | NOVA School of Science and Technology | 6 |
| | | Software Security | Computer Science and Engineering (MSc) | NOVA School of Science and Technology | 6 |
| | | Cybersecurity and Governance | Master's in Law and Security (MSc) | NOVA School of Law | 6 |
| | | Data Protection and Management Law | Master's in Law and Security | NOVA School of Law | 6 |
| | | Cybersecurity | PostGraduate in Smart Cities<br>PostGraduate in Digital Enterprise Management<br>PostGraduate in Information Management and Business Intelligence in Healthcare<br>PostGraduate in Enterprise Information Systems | NOVA Information Management School | 7.5 |
| **CSP008_SA_H:Healthcare sector cyber security** | UPRC | Information Systems Security | Informatics (BSc) | University of Piraeus | 4 |
| | | Information Systems Security Management | Cybersecurity and Data Science (MSc) | | 4 |
| **CSP006_S_H:Network and IoMT Security** | | Information Systems Security | Informatics (BSc) | | 4 |
| | | Information Systems Security Management | Cybersecurity and Data Science (MSc) | | 4 |

## Annex F: Existing program/courses which have been reviewed/complemented/enhanced during WP3

| CSP Module name | Who | Academic course name | Academic program name (BSc/MSc) | University | ECTS |
|---|---|---|---|---|---|
| | | Maritime Information Systems | Informatics (BSc) | | 4 |
| **CSP003_SA_H: Cybersecurity Risk Management and Governance in the Healthcare sector** | | Systems Security Management | Informatics (BSc) | | 3 |
| | | Information Systems Security | Informatics (BSc) | | 4 |
| **CSP001_W_H: Cybersecurity Essentials and Management for Health Sector** | | Information Systems Security | Informatics (BSc) | | 4 |
| | | Information Systems Security Management | Cybersecurity and Data Science (MSc) | | 4 |
| | | Systems Security Management | Informatics (BSc) | | 3 |
| **CSP002_SS_H: Human Factors in Cybersecurity for Health Sector** | TalTech, trustilio, Laurea | Human Factors in Cybersecurity for Health Sector | Masters in Cybersecurity (MSc) | Tallinn University of Technology | 2 |

Table 41. Existing program/courses  which have been reviewed/complemented/enhanced during WP3 (Energy sector).

| CSP Module name | Who | Academic course name | Academic program name (BSc/MSc) | University | ECTS |
|---|---|---|---|---|---|
| **CSP001_C_E: Cybersecurity Essentials and Management for Energy Sector** | LAU, UMA, TALTECH, SGI, PDMFC, trustilio | Information Security Management | Business Information Technology - Cybersecurity (BSC) | Laurea University of Applied Sciences | 5 |
| | | Cybersecurity management | Business Information Technology - Cybersecurity (BSC) | | 5 |
| | | Introduction to Information Security | Business Information Technology - Cybersecurity (BSC) | | 5 |
| | | Information and Cyber Security Management | Business Information Technology - Cybersecurity (BSC) | | 10 |
| | | Introduction to Information Security | Computer Science (BSc.) | University of Malaga | 1 |
| | | Cybersecurity management and protocols | | | 2 |
| | | Information and Cyber Security Management | | | 2 |
| | | Network and application security | | | 1 |
| **CSP004_C_E: Network Protection for Energy Control Systems** | UMA, AIT | Network Security | Computer Engineering (MSc.) | University of Malaga | 4 |
| | | Operation system security | | | 1 |
| | | Network infrastructure security | | | 1 |

Annex F: Existing program/courses which have been reviewed/complemented/enhanced during WP3

| CSP Module name | Who | Academic course name | Academic program name (BSc/MSc) | University | ECTS |
|---|---|---|---|---|---|
| **CSP006_C_E: Cyber Threat Intelligence in the Energy Network** | FCT | Cybersecurity and Governance | Master's in Law and Security (MSc.) | NOVA School of Law | 6 |
| | | Cybercrime | Master's in Law and Security (MSc.) | NOVA School of Law | 6 |
| | | Cybersecurity | PostGraduate in Smart Cities<br>PostGraduate in Digital Enterprise Management<br>PostGraduate in Information Management and Business Intelligence in Healthcare<br>PostGraduate in Enterprise Information Systems | NOVA Information Management School | 7.5 |
| | | Cybersecurity and Data Privacy in Information Management | Executive Program | NOVA Information Management School | 6 |
| **CSP007_C_E: Cybersecurity in Emerging Technologies for Energy** | UNINOVA, LAU | Information Security Management Enterprise | Business Information Technology - Cybersecurity (BSC) | Laurea University of App lied Sciences | 5 |
| | | Enterprise Security and Practitioners | Business Information Technology - Cybersecurity (BSC) | | 5 |
| | | Cybersecurity Working Life Practices | Business Information Technology - Cybersecurity (BSC) | | 2 |
| | | Cybersecurity Hackathon Project | Business Information Technology - Cybersecurity (BSC) | | 2 |

| CSP Module name | Who | Academic course name | Academic program name (BSc/MSc) | University | ECTS |
|---|---|---|---|---|---|
| | | Cybersecurity Project | Business Information Technology - Cybersecurity (BSC) | | 5 |
| | | Network and Application Security | Business Information Technology - Cybersecurity (BSC) | | 5 |
| | | Cybersecurity Analyst | Business Information Technology - Cybersecurity (BSC) | | 5 |
| | | Internet Infrastructure and Security | Business Information Technology - Cybersecurity (BSC) | | 10 |
| | | Introduction to Information Security | Business Information Technology - Cybersecurity (BSC) | | 5 |
| **CSP008_C_E: Critical Energy Infrastructure Security** | UNINOVA, FCT, PDMFC | Network and Computer Systems Security | Computer Science and Engineering (MSc) | NOVA School of Scienc e and Technology | 6 |
| | | Software Security | Computer Science and Engineering (MSc) | NOVA School of Scienc e and Technology | 6 |
| | | Cybersecurity and Governance | Master's in Law and Security | NOVA School of Law | 6 |
| | | Cybersecurity | PostGraduate in Smart Cities<br>PostGraduate in Digital Enterprise Management | NOVA Information Management School | 7.5 |

Annex F: Existing program/courses which have been reviewed/complemented/enhanced during WP3

| CSP Module name | Who | Academic course name | Academic program name (BSc/MSc) | University | ECTS |
|---|---|---|---|---|---|
| | | | PostGraduate in Information Management and Business Intelligence in Healthcare<br>PostGraduate in Enterprise Information Systems | | |
| **CSP009_C_E: Memory-corruption Mechanics** | UCY, FCT | Network and Application Security<br>Introduction to Information Security | Computer Science (BSc) | University of Cyprus | 5 |
| **CSP011_S_E_Cyber_Range_Operation on SCADA** | C2B | Information Security Management Enterprise | Master 2 – M2 : Gestion de la production logistique, Management Maritime et portuaire (MSc) | Université de la cote d'Opale | 2 |
| | | Enterprise Security and Practitioners | | | 5 |
| | | Cybersecurity Working Life Practices | | | 2 |
| | | 4. Network an Application Security | | | 5 |
| **CSP010_S_E: Cybersecurity in Energy** | UPRC | Information Systems Security Management | Cybersecurity and Data Science (MSc) | University of Piraeus | 4 |
| **CSP002_SS_E: Human Aspect of Energy Cybersecurity** | TalTech, trustilio, Laurea | Human Aspects of Energy Cybersecurity | Masters in Cybersecurity (MSc) | Tallinn University of Technology | 2 |