Project No. 101083594 Project start: 2022-12-01
Call: DIGITAL-2021-SKILLS-01 Project duration: 36 months

CyberSecPro

# D2.3
# CyberSecPro Programme Specifications

| Document Identification | |
|---|---|
| Due date | 2023-10-30 |
| Submission date | 2023-23-22 |
| Version | 1.0 |

| | | | |
|---|---|---|---|
| Related WP | WP2 | Dissemination Level | PU |
| Lead Participant | GUF | Lead Author | Ann-Kristin Lieberknecht |
| Contributing Participants | GUF, LAU, TALTECH, TUBS, TUC, UMA, CNR, COFAC, UPRC, MAG, PDMFC, TRUSTILLIO, FCT, UNSPMF | Related Deliverables | D2.1, D2.2, D3.1 |

**Abstract:** The specifications of the CyberSecPro education and training programme will be proposed in this deliverable. The deliverable will reflect the outcomes of task T2.4 and will be the basis for building the CyberSecPro 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. 

## Executive Summary

This deliverable outlines the structure, requirements, and specifications of the CyberSecPro education and training programme. The main findings of this deliverable are as follows:

1. By following four selection criteria (namely market demand, relevance to the European Cybersecurity Skills Framework (ECSF), availability of education and training resources, as well as importance to the effective protection of European cyber infrastructure and systems) ten knowledge areas have been identified that will set the scope of the CyberSecPro education and training programme. By the careful analysis and selection of these knowledge areas, the general structure of the programme is established and direction to the CyberSecPro partners in the continuation of the project provided.
2. The existing education and training offerings by CyberSecPro partners have been mapped to the identified knowledge areas, and relevant training modules have been selected. This ensures that the programme is built upon established resources and expertise.
3. The constraints and requirements for the adoption of 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.
4. A total of 68 user stories and 461 requirements for the implementation of the dynamic curriculum management (DCM) system have been developed. These requirements have been categorised into functional, non-functional, constraint, and supplemental requirements, with different levels of priority. They will serve as the foundation for the subsequent stages of development and implementation of the DCM system.
5. Assessment criteria for the selection of a DCM system have been established, and available systems on the market have been evaluated accordingly. Moodle has been identified as the chosen system. 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 is able to meet the specific needs of the CyberSecPro education and training programme.

By addressing these key findings, the CyberSecPro education and training programme can be designed and implemented effectively, providing a comprehensive and relevant training experience for participants while overcoming any potential challenges

# Document information

## Contributors

| Name | Beneficiary |
|---|---|
| Ann-Kristin Lieberknecht, Atiyeh Sadeghi, Narges Arastouei, Kai Rannenberg | GUF |
| Paresh Rathod, Paulinus Ofem, Leo Johannesberg, Jari Savolainen, Jari Räsänen, Jyri Rajamäki, Rauno Pirinen | LAU |
| Ricardo Gregorio Lugo | TALTECH |
| Cristina Alcaraz, Ruben Rios, Javier Lopez, Antonio Muñoz | UMA |
| Nineta Polemi, Theodoros Karvounidis, Christos Troussas | UPRC |
| Luís Miguel Campos, Nuno Filipe Pedrosa, Carlos Nuno Marques | PDMFC |
| Kitty Kioskli | TRUSTILLIO |
| Danijela Boberic | UNSPMF |
| Pinelopi Kyranoudi, Charambos Mitropoulos, Markos Kimionis, Evripidis Sotiriadis | TUC |
| Vasco Delgado-Gomes, Ruben Costa, Paulo Figueiras | UNINOVA |

## Reviewers

| Name | Beneficiary |
|---|---|
| Gregor Langner | AIT |
| Fabio Martinelli | CNR |

## History

| Version | Date | Contributor(s) | Comment(s) |
|---|---|---|---|
| 0.01 | 2023-03-13 | Ann-Kristin Lieberknecht | 1st Draft |
| 0.02 | 2023-03-17 | Ann-Kristin Lieberknecht, Nineta Polemi, Paresh Rathod | High-level review with improved ToC |
| 0.03 | 2023-05-25 | Kitty Kioskli | Section added |
| 0.04 | 2023-06-08 | Cristina Alcarez, Ruben Rios | Several sections added |
| 0.05 | 2023-06-08 | Theodoros Karvounidis, Christos Troussas | Several sections added |
| 0.06 | 2023-06-13 | Theodoros Karvounidis | Minor changes and additions |
| 0.07 | 2023-07-04 | Cristina Alcarez, Ruben Rios | Minor changes and additions |
| 0.08 | 2023-07-15 | Cristina Alcarez, Ruben Rios, Kitty Kioskli | Addressing comments |
| 0.09 | 2023-07-24 | Cristina Alcarez, Ruben Rios, Nineta Polemi | Addressing comments |
| 0.10 | 2023-08-21 | Ann-Kristin Lieberknecht | Several sections added |
| 0.11 | 2023-08-31 | Ann-Kristin Lieberknecht, Per Håkon Meland, Nineta Polemi, Paresh Rathod, Bruno Bender | Addressing comments |
| 0.12 | 2023-09-18 | Atiyeh Sadeghi | Editorial improvements |
| 0.13 | 2023-09-19 | Ann-Kristin Lieberknecht | Several sections added |
| 0.14 | 2023-09-25 | Paresh Rathod, Paulinus Ofem, Ann-Kristin Lieberknecht | Several sections added |
| 0.15 | 2023-09-30 | Ann-Kristin Lieberknecht | Editorial Changes |
| 0.16 | 2023-10-01 | Ann-Kristin Lieberknecht | Sections added and Editorial Changes |
| 0.17 | 2023-10-01 | Paresh Rathod, Paulinus Ofem, Ann-Kristin Lieberknecht | Several sections added and revised |
| 0.18 | 2023-10-03 | Ann-Kristin Lieberknecht | Minor improvements |
| 0.19 | 2023-10-05 | Cristina Alcaraz | Addressing comments |

| | | | |
|---|---|---|---|
| 0.20 | 2023-10-06 | Narges Arastouei, Arman Khan, Christos Troussas, Carlos Nuno Marques | Ref, Table of Content & DCM |
| 0.21 | 2023-10-06 | Ann-Kristin Lieberknecht | Editorial Changes |
| 0.22 | 2023-10-24 | Ann-Kristin Lieberknecht, Javier Lopez, Antonio Muñoz, Jeldo Meppen, Fabio Martinelli, Gregor Langner | Addressing review feedback, sections added |
| 0.23 | 2023-10-30 | Ann-Kristin Lieberknecht, Arman Khan | Editorial Changes |
| 0.24 | 2023-10-31 | Ann-Kristin Lieberknecht, Arman Khan | Editorial Changes |
| 0.25 | 2023-11-01 | Ann-Kristin Lieberknecht, Arman Khan | Editorial Changes |
| 0.26 | 2023-12-18 | Ann-Kristin Lieberknecht, Talha Aamir, Stefan Schauer, Martin Latzenhofer | Adressing review feedback |
| 1.0 | 2023-12-22 | Ann-Kristin Lieberknecht | Final check, layout refinement and submission process |

# Table of Contents

**List of Figures**



## List of Tables

# List of Acronyms

| | | |
|---|---|---|
| *A* | **AI** | Artificial Intelligence |
| | **APIs** | Application Programming Interfaces |
| | **AR** | Augmented Reality |
| *C* | **CA** | Cybersecurity Architect |
| | **CBI** | Computer-based instruction |
| | **CE** | Cybersecurity Educator |
| | **CISO** | Chief Information Security Officer |
| | **CM** | Cybersecurity Management |
| | **CMS** | Curriculum Management System |
| | **CTIS** | Cyber Threat Intelligence Specialist |
| | **CTM** | Cybersecurity Threat Management |
| *D* | **DCM** | Dynamic Curriculum Management |
| | **DFI** | Digital Forensic Investigator |
| *E* | **e-CF** | European e-Competence Framework |
| | **ECSF** | European Cybersecurity Skills Framework |
| | **ECTS** | European Credit Transfer and Accumulation System |
| | **EQF** | European Qualifications Framework |
| | **ESCF** | European Cybersecurity Skills Framework |
| | **EU** | European Union |
| *G* | **GDPR** | General Data Protection Regulation |
| *H* | **HEI** | Higher Education Institutes |
| | **HIPAA** | Health Insurance Portability and Accountability Act |
| *I* | **ICT** | Information and Communications Technology |
| | **IDS** | Intrusion Detection Systems |
| | **ILS** | Integrated Learning Systems |

| | | |
|---|---|---|
| | **IoT** | Internet of Things |
| | **IPS** | Intrusion Prevention Systems |
| | **ISO** | International Organization for Standardization |
| | **IT** | Information Technology |
| | **IR** | Incident response |
| *L* | **LDAP** | Lightweight Directory Access Protocol |
| | **LMS** | Learning Management System |
| | **LTI** | Learning Tools Interoperability |
| *M* | **MOOC** | Massive Open Online Courses |
| *P* | **PPPs** | Public Private Partnerships |
| *R* | **ROI** | Return on investment |
| *S* | **SAML** | Security Assertion Markup Language |
| | **SCORM** | Sharable Content Object Reference Model |
| | **SIEM** | Security Information and Event Management |
| | **SIS** | Student Information Systems |
| | **SLAs** | Service Level Agreements |
| | **SMEs** | Small and Medium-sized Enterprises |
| | **SSL** | Secure Sockets Layer |
| | **SSO** | Single Sign-On |
| *T* | **TLS** | Transport Layer Security |
| *U* | **UDL** | Universal Design Principles |
| *V* | **VR** | Virtaul Reality |
| *X* | **xAPI** | Experience API |

# Glossary of Terms

*C* **CyberSecPro training programme**

will consist of training modules that can be offered individually or as a package; it will not lead to any certification or 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.

**CyberSecPro 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.

**CyberSecPro syllabus**

Every training module will be accompanied by a syllabus that will 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).

A standard template for a CyberSecPro syllabus will be finalised in D4.1 ('CyberSecPro training Operational Plan'), and it will be used in all CyberSecPro training modules.

**CyberSecPro training material**

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

**CyberSecPro sector-specific training modules**

CyberSecPro training modules that will concentrate on the sectors of health, maritime, and energy. 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.

A standard template for a CyberSecPro syllabus will be finalised in D4.1 and it will be used in all CyberSecPro training modules.

**CyberSecPro knowledge areas**

The knowledge areas 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.

**CyberSecPro practical skill**

The initial studies confirm the challenges of interpreting the knowledge areas, skills, and competencies differently across EU nations and organisations. Therefore, CyberSecPro 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”.

**CyberSecPro competence**

The initial studies confirm the challenges of interpreting the knowledge areas, skills, and competencies differently across EU nations and organisations. Therefore, CyberSecPro 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.”

**CyberSecPro training tools**

Training tools that will be used in the training of the CyberSecPro modules (the assessment of the various tools, selection and portfolio will occur in T.2.3).

**CyberSecPro training format**

CyberSecPro training format describes the way how modules will be provided ondemand, web-based, live online, In person, hybrid/mix,

**CyberSecPro Dynamic Curriculum Management System**

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 DCM integration. It will entail the entire curriculum creation, evaluation, review, approval, and promotion processes. regulation compliance (e.g. GDPR).

The main requirements of the CyberSecPro DCM will be flexibility and responsiveness to the continuously changing cybersecurity market needs. Overall, CyberSecPro Dynamic Curriculum Management (DCM): The online Dynamic Curriculum Management (DCM) is an online tool that 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.

# 1 Introduction

## 1.1 Background

The issue of cybersecurity poses a significant and ongoing challenge for companies and industries across all sectors. Extensive research and market analyses have consistently highlighted a growing shortage of qualified professionals in the cybersecurity field, creating alarming concerns within both the private and public sectors. As a response, the CyberSecPro project has been established to address this issue.

The main objective of the CyberSecPro project is to facilitate the practical development of cybersecurity skills among professionals, trainers, and educators. By focusing on collaborative, multi-modal, and agile methodologies, this programme aims to bridge the gap between academic qualifications, real-world work experience, and the high-demand cybersecurity skills essential in today's rapidly evolving digital landscape.

The core of the project focuses on the development of the agile CyberSecPro professional cybersecurity practical and hands-on education and training programme. Through this program, CyberSecPro aims to develop a proficient workforce that can successfully tackle cybersecurity challenges in both the European Digital Single Market and industries. By cultivating an ecosystem that promotes practical skill development and knowledge sharing, this project aims to strengthen cybersecurity defences and advance the resilience of organisations operating in the digital age.

## 1.2 Scope

With the increasing prevalence and sophistication of cyber threats, the need for effective cybersecurity training programmes has become paramount. This deliverable aims to address this need by developing the specifications for the CyberSecPro education and training programme. The specifications refer to both functional and technical aspects, that will be refined within this deliverable. The outcome of this deliverable will set the foundation for the planning, organisation and implementation of the programme, ensuring an effective execution of all project milestones and objectives.

On the functional side, this deliverable will focus on outlining the general structure of the programme. This will be achieved by analysing and selecting the most relevant knowledge areas as well as identifying the potential education and training modules offered within these knowledge areas. Additionally, selected pedagogical approaches for conducting the education and training modules will be investigated. These approaches can be utilised in WP3 and WP4 to increase the quality and foster the continuous improvement and development of training modules.

On the technical side, an analysis of various barriers, constraints, and requirements will be conducted. These include technical, business, societal, legal, and educational challenges that Higher Education Institutes and Industrial Partners may face when adopting and implementing the programme and its modules. This analysis will equip the CyberSecPro consortium with the necessary information to address potential obstacles and create strategies to ensure successful implementation. However, it is important to acknowledge that not all barriers can be resolved by the consortium as certain factors are beyond their control or may excessively burden the project's development. However, by identifying these barriers, the consortium will be better equipped to steer the project in the right direction and potential solutions may arise along the way.

Furthermore, the specifications of the CyberSecPro Dynamic Curriculum Management (DCM) system will be analysed. To ensure the program's effectiveness, user stories will be developed, outlining the requirements for the DCM system. While comprehensive requirement analysis serves as a strong foundation, it is important to recognise that these requirements can only be preliminary. Following an agile approach, the implementation phase provides an opportunity for further refining, adapting, and supplementing the requirements based on emerging system insights, technical challenges, and stakeholder inputs. By embracing the potential for evolving requirements, the DCM system can be better tailored to meet the evolving needs and effectively support the project’s objectives. In a next step,

assessment criteria for the selection of DCM system will be presented, and existing solutions analysed accordingly. Finally, the requirements will be matched against the chosen DCM systems, providing a comprehensive overview of the features and capabilities available. This will lay the foundation for the work on the DCM system in WP3.

### 1.2.1 Relationship with other Work Packages

This deliverable builds upon the work done in D2.1 “Cybersecurity Market Skills and Competencies Analysis” and D2.2 “Practical cybersecurity skills offered in EU Academic Programmes”. The selection of knowledge areas has been influenced by the findings of both deliverables. The identified competencies and skills required by the market, as highlighted in D2.1 and the analysis of cybersecurity courses conducted in D2.2, have been taken into consideration when determining the knowledge areas.

The selected training modules within these knowledge areas will form the foundation for T3.1, which focuses on the development of the training programme. Additionally, the requirements for the DCM system that are developed in this deliverable will be the basis for T3.2, in which the DCM system will be implemented.

### 1.2.2 Purpose and Objective

Developing the specifications of the CyberSecPro education and training programme prior to its implementation is crucial for ensuring its success and effectiveness. Therefore, by carefully analysing and selecting the most relevant knowledge areas and education and training modules, the program's general structure is established in this deliverable. This provides direction not only to CyberSecPro partners in the continuation of the project, but also to trainers and learners, enabling them to focus on achieving the intended goals. Furthermore, by thoroughly investigating key pedagogical aspects, the quality and efficacy of the education and training modules throughout the project can be fostered.

Additionally, the process of developing programme specifications involves identifying potential barriers and constraints to its adoption. By recognising these challenges beforehand, CyberSecPro can develop strategies to overcome them and take them into consideration during the program's design and implementation. This proactive approach to addressing obstacles creates a more effective learning environment and ensures that potential roadblocks do not hinder the program's progress.

Furthermore, having a comprehensive understanding of the design and functionality requirements of the DCM system is vital for the success of the CyberSecPro education and training programme. It is crucial to determine the specific features and capabilities that trainers, learners, and institutions should have within the CyberSecPro programme. This knowledge not only guides the platform selection process but also helps identify areas where customisation may be needed. By analysing the requirements in detail, the set-up process for the CyberSecPro education and training programme can be expedited, ensuring a seamless implementation of the necessary systems.

Overall, developing specifications for a training programme before its implementation fosters a well-organised and efficient learning experience. It ensures clarity in programme design, selection of an appropriate platform, and understanding of potential challenges. This approach facilitates smooth implementation and increases the likelihood of meeting the training program's objectives of offering a practical and hands-on cybersecurity education and training programme.

# 2 CyberSecPro Knowledge Areas

## 2.1 Introducing Knowledge Areas

As recommended by ENISA[1] and many other studies, further collaboration among Higher Education Institutes (HEI) and the private sector is needed in order to address the cybersecurity market challenges and the associated industrial demands. The current academic programmes, with their static curricula, do not provide the dynamic capabilities and emerging skills needed in the market. The digital transformation imposes the HEIs to enhance their role in preparing the new generation workforce or in upskilling the existing one, putting also in practice EU ethical and democratic principles and rights. For this HEIs need to become the main providers of cybersecurity dynamic capabilities and practical skills. Therefore, CyberSecPro is developing flexible practical education and training modules (e.g. courses, ad-hoc seminars, fast courses, summer schools, workshops, cyber exercises, hackathons, and cyber games) in specific knowledge areas that are needed in the EU Digital Single Market and EU industries. Combined they represent the agile CyberSecPro professional cybersecurity practical and hands-on education and training programme that will complement, align, support and advance the existing academic programmes by linking innovation, research, industry, academia and small and medium-sized enterprises support.

In the upcoming chapter, we will determine the knowledge areas that are essential for the CyberSecPro education and training programme. In the context of the CyberSecPro project, we understand a Knowledge area as a specific field or domain of expertise that encompasses a set of concepts, principles, and practices within a particular discipline or industry – in our case cybersecurity. Each Knowledge area focuses on a distinct aspect of knowledge and seeks to develop and advance understanding in that specific area. The careful selection of specific knowledge areas is pivotal in guaranteeing the program's quality and, consequently, its success.

The rest of this chapter is structured as following: First, the methodology for the selection of knowledge areas will be set out. Second, a comprehensive evaluation of the main knowledge areas obtained from the state-of-the-art analysis and market demand survey conducted in D2.1 will be presented. This evaluation will take into consideration the existing training offerings provided by both academic and industrial partners at CyberSecPro that were thoroughly examined in D.2.2. Furthermore, it will also align with the European Cybersecurity Skills Framework (ECSF) in order to assess the suitability of these knowledge areas. Third, further considerations about additional knowledge areas will be discussed. Last, the final set of Cybersecurity knowledge areas for the CyberSecPro education and training will be proposed, and limitations discussed.

## 2.2 Methodology of Selection

### 2.2.1 Selection Criteria

The careful selection of specific knowledge areas is pivotal in guaranteeing the program's quality and, consequently, its success. To maximise the potential impact of the CyberSecPro project, a multi-level selection system was carefully chosen. The following selection criteria were considered:

[1] ENISA report, "Addressing the EU cybersecurity skills shortage and gap through higher education." (2021). [online] Available at: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport.


Figure 1: Selection criteria for CyberSecPro knowledge areas

At the core of the selection systematic are the state-of-the-art analysis and the market demand survey that were conducted in the context of *D2.1 Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analysis*. The state-of-the-art analysis conducted in D.2.1 revealed that cybersecurity knowledge and skills are applicable and required across all sectors of the economy. The CSP study also consolidates that cybersecurity is a cross-sectoral subject, and cybersecurity knowledge and skills are essential for all sectors, as they are necessary to protect organisations from increasingly sophisticated cyberattacks. The D2.1 analysis also identified and prioritised 18 cybersecurity knowledge and skills gaps across Europe defined as the gap between European cybersecurity workforce market demand and HEIs' academic offerings. The analysis also confirms that educational cybersecurity offerings do not adequately cover cybersecurity practical and working-life skills. These knowledge and skills gaps are a significant challenge for the cybersecurity workforce, and CyberSecPro aims to address them. These cybersecurity knowledge and skills shortages remain a priority for the European cybersecurity workforce, as reported in various ENISA publications. CyberSecPro, through the current study, aims to develop and enhance cybersecurity training offerings, especially for CSP consortium members.

The market demand survey contained multiple-choice questions on the industry's relevant job roles and open-ended questions on the knowledge areas and hands-on skills needed by cybersecurity professionals. In total, 243 responses from various European countries were collected. It is crucial to recognise that although the number of responses for this survey is substantial, it does not necessarily provide a representative sample but rather indicates a trend. However, considering that the survey is just one aspect used to select the knowledge areas, this limitation does not pose a problem. The responses were inspected and categorised to identify patterns and trends in the data, using descriptive statistics for multiple-choice questions, and content analysis for open-ended questions. One of the findings was the difficulty in distinguishing between knowledge areas and skills, as numerous instances of overlap were consistently observed. Complicating matters further, different interpretations and understandings of skills are observed among EU countries and organisations. Consequently, it was determined that knowledge areas and skills should be considered together and, moving forward, only referred to as knowledge areas. Another finding was, that respondents from the three specific sectors health, energy, and maritime valued similar knowledge areas than respondents from other sectors. However, due to the limited sample size, a reliable conclusion about the exact priorities for each sector could not be drawn. Consequently, the selection of knowledge areas focuses on identifying the most crucial knowledge areas across sectors rather than sector-specific ones. The survey suggests that general knowledge areas chosen in the end are highly likely to fulfil the demand in the specific sectors as well.

Next to the market demand survey, the second selection criterion is the alignment to the European Cybersecurity Skills Framework (ECSF). The ECSF is a comprehensive framework developed by the European Union to address the increasing challenges posed by cyber threats and ensure a skilled and Knowledgeable workforce in the field of cybersecurity. It provides a common language and structure for describing, learning, and assessing cybersecurity skills across Europe. By mapping the survey results

to the ECSF job roles, a common terminology can be assured and the relevance of the knowledge areas confirmed.

To further enhance the selection process, the availability of resources within the CyberSecPro consortium is determined as a crucial criterion. The overarching goal of the CyberSecPro project is to integrate the collective expertise of all partners (as presented in D.2.2) to benefit from the combined competence. By doing so, the project strives to efficiently address the ever-evolving requirements for cybersecurity workforce knowledge. By emphasising existing competences, the project guarantees a superior quality and maximises its potential impact.

Finally, the importance to the effective protection of European cyber infrastructures and systems was considered. The addition of this criterion introduces discussion topics that may have been inadequately addressed or overlooked. This inclusion opens up opportunities for considering important aspects that have been previously neglected or omitted in the analysis.

### 2.2.2 Selection Process

The selection process for knowledge areas in the CyberSecPro education and training programme involves four rounds, as depicted in Figure 2. Firstly, in accordance with the approach outlined in D2.1, all knowledge areas mentioned more than 40 times are considered in the initial round of selection. In the second round, the remaining knowledge areas are evaluated against the ECSF to determine their relevance and align them with the European commission's initiative for a more effective and cohesive effort. The terminology for each Knowledge area is adjusted accordingly.

Next, an assessment is made of the availability of existing education and training resources within the CyberSecPro consortia members and partners' network. This data is gathered in the context of *D2.2 Blended CyberSecPro technological training interactive technologies and academic practice*. In this deliverable, available courses have been clustered according to their topic. The clusters with three and more courses are: Risk Management and Governance (14 courses), Network Security (9 courses), Malware and Attack Technologies (8 courses), Applied Cryptography (8 courses), Privacy and Online Rights (6 courses), Maritime Informatics (5 courses), Software Security (5 courses), Authentication, Authorisation, and Accountability (4 courses), Security Operations & Incident Management (3 courses), Forensics (3 courses), and Operating Systems & Virtualisation Security (3 courses). These clusters of courses are mapped to all potential knowledge areas. Mapping each course individually to every potential Knowledge area would possibly provide a more accurate result. However, by comparing the main clusters of courses, we can still gain valuable insights into the course supply without having to analyse each course one by one. Therefore, the advantage of time and resources saved in not having to evaluate all courses for every possible Knowledge area individually outweighs the necessity for such detailed analysis in this specific context. Accordingly, in order to reduce complexity, this simplified approach is chosen. knowledge areas without corresponding courses are filtered out, as the rationale behind this is to ensure that consortium members can concentrate on leveraging existing knowledge and competences to guarantee the quality of courses and ultimately achieve the overall success of the CyberSecPro education and training programme.

Lastly, the final round of selection involves the introduction of new discussion topics based on survey comments and the considerations of the CyberSecPro consortium. This qualitative approach serves as a valuable counterbalance to the previous quantitative metrics, addressing any potential shortcomings in the survey. This approach ensures that no significant Knowledge area is overlooked. These new topics are evaluated in the context of the previously selected knowledge areas to determine their relevance and whether they are already adequately covered.

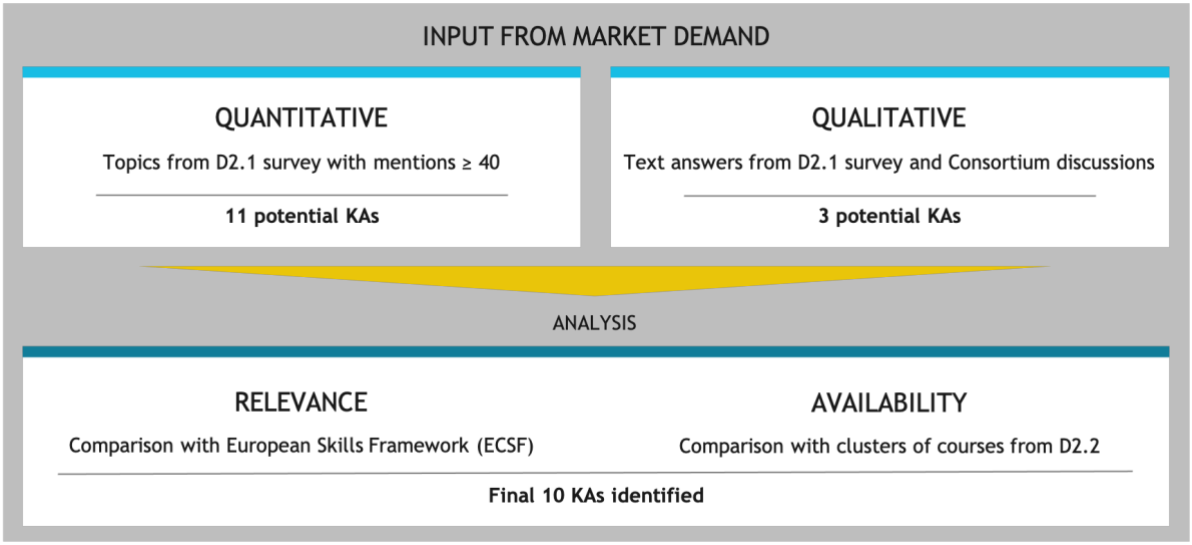



Figure 2: Selection process for CyberSecPro knowledge areas

## 2.3 Analysis of Knowledge Areas

### 2.3.1 Knowledge Areas derived from D2.1

In the context of *D2.1 Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analysis* a state-of-the-art analysis and a survey among 235 cybersecurity professionals was conducted. In the context of the survey, the following knowledge areas were identified in descending order of number of observations (compare with *D2.1, table 21*):

Table 1: Knowledge areas from market demand survey

| **Knowledge Area** | **No of observations** | **Keywords** |
|---|---|---|
| Ethical Hacking and Penetration Testing | 192 | Penetration Testing/ Ethical Hacking/ Defensive Practitioners/ Offensive Security/ Vulnerability Assessment/ Vulnerability Analysis |
| Cybersecurity Tools and Technologies | 187 | Cybersecurity Tools/Cybersecurity Technologies |
| Cybersecurity Management Systems: CyberSecurity Management and Processes | 111 | Cybersecurity Management, Cybersecurity Management Systems, Cybersecurity Processes |
| Cybersecurity Principles | 81 | Cybersecurity Principles |
| Cybersecurity Threat Management: Threat Awareness, Threat Knowledge, Threat Assessment, Threat Intelligence, Threat Detection | 78 | Cybersecurity Threat Awareness/Threat Intelligence/Threat Detection/Threat Understanding/Threat Knowledge |
| Cybersecurity Risk Assessment and Risk Management | 76 | Cybersecurity Risk Assessment/Risk Management |

| | | |
|---|---|---|
| Emerging Technologies | 65 | Emerging Technologies |
| Cybersecurity Regulations and Compliance | 58 | Cybersecurity Regulations/Cybersecurity Compliance/Compliance |
| Cybersecurity education and training | 49 | education and training/education and training Skills |
| Incident Response | 49 | Incident Response |
| Communications and Network Security: Network Security Controls | 48 | Communication and Network Security/Network Security Control |
| Cybersecurity Forensics | 38 | Cybersecurity Forensics |
| Cloud Security | 37 | Cloud Security |
| Cybersecurity for Artificial Intelligence and Machine Learning | 32 | Cybersecurity for Artificial Intelligence and Machine Learning/Artificial Intelligence |
| Legal and Auditing Training | 27 | Legal Training/Auditing |
| Cybersecurity Architecture | 24 | Cybersecurity Architecture |
| Cybersecurity Engineering | 22 | Cybersecurity Engineer/DevSecOps/DevOps |
| Network and System Administration | 21 | Network and System Administration |
| Technical Skills | 18 | Technical Skills |
| Software Security | 17 | Software Security |
| Analysis and Critical Thinking (soft/professional skills) | 16 | Analysis and Critical Thinking (soft/professional skills) |
| Programming Skills | 14 | Programming Skills |
| Communication and Teamwork | 13 | Communication and Teamwork |
| Operating Systems | 12 | Operating Systems |
| Software Design Skills | 11 | Software Design Skills |
| Data Protection and Security | 9 | Data Protection and Security |

It is important to note, that some of the knowledge areas were primed by a picture that was given as an example for knowledge areas (see [1]). These are marked in orange in Table 1. As the survey responses may be influenced by the picture and the sample obtained may not be fully representative, it is crucial to consider the answers in their proper context. Nevertheless, the survey offers a valuable insight into emerging trends and can thus serve as an initial foundation for analysing potential knowledge areas. For this the approach in D2.1 was followed and only knowledge areas with over 40 observations considered for the first step in the analysis. Figure 3 provides an overview of knowledge areas mapped against the

ECSF job roles and CyberSecPro course portfolio. In the following, each knowledge areas will be discussed individually.


Figure 3: Picture given in survey as example for knowledge areas [1]

Table 2: Mapping knowledge areas from survey, ECSF and CyberSecPro course portfolio

| Market Demand: Survey | Relevance: ECSF | Availability: Course Portfolio | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Knowledge Areas in high demand | | Risk Management and Governance (14) | Network Security (9) | Malware and Attack Technologies (8) | Applied Cryptography (8) | Privacy and Online Rights (6) | Maritime Informatics (5) | Software Security (5) | Authentication, Authorisation and Accountability (4) | Security Operations & Incident Management (3) | Forensics (3) | Operating Systems & Virtualisation Security (3) |
| Ethical Hacking and Penetration Testing (192) | Penetration Tester | | | x | | | | | | | | |
| Cybersecurity Tools and Technologies (187) | | | | | | | | x | x | | | x |
| Cybersecurity Management Systems: CS Management and Processes (111) | Chief Information Security Officer (CISO) | x | | | | | | | | | | |
| Cybersecurity Principles (81) | | | | | | | | | | | | |
| Cybersecurity Threat Management / Security Operations Center (78) | Cyber Threat Intelligence Specialist, Cyber Incident Responder | | | | | | | | | x | x | |
| Cybersecurity Risk Assessment and Risk Management (76) | Cybersecurity Risk Manager | x | | | | | | | | | | |
| Emerging Technologies (65) | | | | | | | | | | | | |
| Cybersecurity Regulations and Compliance (58) | Cyber Legal, Policy & Compliance Officer | x | | | | | | | | | | |
| Cybersecurity Education and Training (49) | Cybersecurity Educator: Improves cybersecurity knowledge, skills and competencies of humans. | | | | | | | | | | | |
| Incident Response (49) | Cyber Incident Responder | | | | | | | | | x | | |
| Network and Communications Security (48) | Cybersecurity Architect: Plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls. | | x | | | | | | | | | |

Penetration Testing

In the survey, *Ethical Hacking and Penetration Testing* was rated high in terms of knowledge areas in demand. In total, respondents named "Penetration testing/Ethical hacking/Defensive Practitioners/Offensive Security/Vulnerability assessment/Vulnerability analysis" 192 times as important, which is the highest result for a Knowledge area, making it the top most mentioned Knowledge area. However, it is noteworthy that this knowledge areas was primed by the example picture. *Ethical Hacking and Penetration Testing* directly relates to the ECSF role of Penetration tester, who simulates real-world attacks to assess the effectiveness of security controls. In doing so cybersecurity vulnerabilities can be uncovered and their criticality assessed. In accordance with the terminology used in the ECSF, henceforward we will refer to the Knowledge area as *Penetration Testing*. The increasing sophistication of cyberattacks has resulted in a high market demand for penetration testing skills, as indicated by the findings in the CyberSecPro D2.1 outcome, numerous EU studies, and reports. Organisations are recognising the need to protect themselves from such attacks and are embracing penetration testing as a critical component of their cybersecurity strategy. As a result, there is an escalating search for qualified penetration testers who can effectively assess their security posture. Given the current scenario, the market demand for penetration testing is expected to not only remain high but also continue growing in the future. The CyberSecPro consortium offers in total 8 courses that cover *Penetration Testing*:

Table 3: CyberSecPro courses covering Penetration Testing

| **Partner** | **Course** | **Department** |
|---|---|---|
| UPRC | Information Systems Security | Department of Informatics |
| UPRC | Malware Analysis, MSc | Department of Informatics |
| LAU | Enterprise Security and Practitioners | ICT & Cybersecurity |
| TalTech | Cyber Defence Monitoring Solutions | Department of Software Sciences, MSc |
| PDMFC | Vulnerability Assessment & Management | Research and Development |
| PDMFC | Penetration Testing | Research and Development |
| UMA | Malware Analysis | Computer Science, MSc |
| Focal Point | Penetration Testing | |

In conclusion, the CyberSecPro criteria Market Demand, Relevance to ECSF, and Course Availability are met, which is why *Penetration Testing* is included in the list of CyberSecPro knowledge areas.

Cybersecurity Tools and Technologies

The survey revealed a significant preference for *Cybersecurity Tools and Technologies*, with a high number of respondents (187) ranking them as an important Knowledge area. However, it is important to acknowledge that this term has been primed by the example picture. Nonetheless, these findings support a high demand for tools and technologies in the cybersecurity field. While the survey did not require participants to specify their answers, it can be assumed that the majority of respondents were referring to commonly used tools such as antivirus software, firewalls, intrusion detection systems, encryption software, and more. This range of *Cybersecurity Tools and Technologies* highlights their

diverse applications within the field of cybersecurity. As a result, it is not possible to relate this field to one specific job role within the ECSF. The CyberSecPro consortium covers *Cybersecurity Tools and Technologies* in the context of different courses:

Table 4: CyberSecPro courses covering Tools and Technologies

| **Partner** | **Course** | **Department** |
|---|---|---|
| UPRC/ Trustilio | Software Security | Department of Informatics, MSc/ joined training |
| LAU | Fundamentals of Programming | ICT & Cybersecurity |
| UCY | Software Analysis | Computer Science |
| FCT | Software Security | Department of Informatics |
| UMA | Secure Coding | Computer Science, MSc |
| GUF | Information & Communication Security | Economics & Business |
| UMA | Digital Identity and Privacy | Computer Science |
| UMA | Security in Services and Applications | Computer Science |
| UMA | Information Security | Computer Science |
| LAU | Data Networks and Information Security | ICT & Cybersecurity |
| LAU | Information Management and Databases | ICT & Cybersecurity |
| UMA | Design and Configuration of Secure Network Systems | Computer Science |

In summary, *Cybersecurity Tools and Technologies* ranked high in the survey and is often covered within courses of the CyberSecPro consortium. The authors do not interpret the lack of *Tools and Technologies* within the ECSF as proof for the irrelevance of the knowledge areas. Instead, the CyberSecPro state-of-the-art analysis and market demand survey confirm that the wide range of applications emphasises the significance of *Tools and Technologies* in the implementation of cybersecurity. Furthermore, the studies also found that cybersecurity tools and technologies are essential for implementing effective cybersecurity measures. Therefore, the market demand for cybersecurity tools and technologies is likely to continue to grow in the coming years. Therefore, *Cybersecurity Tools and Technologies* are included as a Knowledge area in the CyberSecPro education and training programme.

Cybersecurity Management

With a total of 111 mentions, *Cybersecurity Management Systems: CS Management and Processes* was the third most common answer with regards to knowledge areas in demand. Within this category the answers “Cybersecurity management, cybersecurity management systems, cybersecurity processes” were included. The high amount of mentions is most likely biased by the example picture given in the survey to explain knowledge areas. Within the ECSF, *Cybersecurity Management Systems: CS Management and Processes* relate best to the role of Chief Information Security Officer (CISO), who manages an organisation’s cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected. Accordingly, this Knowledge area is

henceforward referred to as *Cybersecurity Management. Cybersecurity Managemen*t is covered in 14 courses within the CyberSecPro consortium:

Table 5: CyberSecPro courses covering Cybersecurity Management

| **Partner** | **Course** | **Department** |
|---|---|---|
| UPRC | Security Governance | Department of Informatics |
| UPRC | Security Policies and Security Management | Department of Digital Systems |
| UPRC | Operational Research | Department of Business Administration |
| UPRC | Information Security Governance, MSc | Department of Informatics |
| UPRC/FP/ Trustilio/ TUC | Cybersecurity Hands-On-Training (CyberHOT) | Joined series of seminars |
| UPRC | Cybersecurity Policies and Practices in the EU - for non-IT Experts | |
| LAU | Information Security Management | ICT & Cybersecurity |
| LAU | Risk Management | |
| PDMFC | Introduction to Risk Management using Eramba or Simple Risk Open Source Software | Research and Development |
| PDMFC | ISO/IEC 27001 | Research and Development |
| FCT | Globalisation and Security Risks | NOVA Information Management Schools |
| MAG | Cyber Security Specialist | Maggioli Academy |
| MAG | Project Management | Maggioli Academy |
| Trustilio | Human Factors in Cybersecurity Management | |

To conclude, the criteria Market Demand, Relevance to ECSF, and Course Availability are met. Therefore, *Cybersecurity Management* is included as a CyberSecPro Knowledge area.

Cybersecurity Principles

When asked about the most urgent cybersecurity knowledge areas, participants mentioned *Cybersecurity Principles* a total of 81 times. This ranked as the fourth most common answer. This term again was primed by a picture that was provided as an example for knowledge areas, which may have influenced participants' responses. It is likely that when mentioning Cybersecurity Principles, participants are referring to general principles such as avoiding dependency on single instances, following the principle of least privilege in access control, or keeping the key, rather than the algorithm,

secret in cryptography. Since *Cybersecurity Principles* is a broad and generic Knowledge area, it cannot be directly linked to a specific ECSF job role. Similarly, the CyberSecPro consortium does not offer a specific course solely dedicated to Cybersecurity Principles. Instead, these principles are covered across all the courses offered by the consortium, i.e. courses in the field of *Cybersecurity Management*. Therefore, it is omitted as independent Knowledge area.

Cybersecurity Threat Management

*Cybersecurity Threat Management / Security Operations Centre* was mentioned 78 times for important cybersecurity knowledge areas. This corresponds to the fifth most common answer for cybersecurity skills. Keywords included were "Cybersecurity threat awareness/Threat intelligence/Threat detection/Threat understanding/Threat knowledge". Within the ECSF it relates to the Digital Forensics Investigator and the Cyber Threat Intelligence Specialist. While the former ensures that the investigation reveals all digital evidence to prove the malicious activity, the latter collects, processes, and analyses data and information to produce actionable intelligence reports and disseminate them to target stakeholders. For simplicity, it will be referred to as *Cybersecurity Threat Management* henceforward. Cybersecurity Threat Management (CTM) is a proactive approach to preventing attacks from happening, while incident response (IR) is a reactive approach to dealing with attacks that have already happened. Both CTM and IR are essential for effective cybersecurity. Within the CyberSecPro consortium, several courses cover *Cybersecurity Threat Management*:

Table 6: CyberSecPro courses covering Cybersecurity Threat Management

| **Partner** | **Course** | **Department** |
|---|---|---|
| LAU | Management of Cybersecurity | ICT & Cybersecurity |
| UPRC | Digital Forensics, MSc | Department of Informatics |
| UMA | Information Security and Computer Forensics | Computer Science |
| UMA | Computer Forensics | Computer Science, MSc |

Overall, the CyberSecPro criteria Market Demand, Relevance to ECSF, and Course Availability are met. Most essentially, there is a growing need for skilled cybersecurity professionals who can manage and mitigate cyber threats. Cybersecurity Threat Management is essential for organisations of all sizes to have a strong understanding of this discipline. Consequently, *Cybersecurity Threat Management* is included to the list of CyberSecPro knowledge areas.

Cybersecurity Risk Management

*Cybersecurity Risk Assessment and Management* were mentioned 76 times as important Knowledge area. It relates best to the ECSF job role of Cybersecurity Risk Manager. The Cybersecurity Risk Manager manages the organisation's cybersecurity-related risks aligned to the organisation's strategy and develops, maintains and communicates the risk management processes and reports. In accordance with the terminology used in the ECSF, henceforward we will refer to the Knowledge area as *Cybersecurity Risk Management.* In the CyberSecPro project, various courses dealing with *Cybersecurity Risk Management* are offered by consortium members:

Table 7: CyberSecPro courses covering Cybersecurity Risk Management

| **Partner** | **Course** | **Department** |
|---|---|---|

| | | |
|---|---|---|
| UPRC | Security Governance | Department of Informatics |
| UPRC | Security Policies and Security Management | Department of Digital Systems |
| UPRC | Operational Research | Department of Business Administration |
| UPRC | Information Security Governance, MSc | Department of Informatics |
| UPRC/FP/ Trustilio/ TUC | Cybersecurity Hands-On-Training (CyberHOT) | Joined series of seminars |
| UPRC | Cybersecurity Policies and Practices in the EU - for non-IT Experts | |
| LAU | Information Security Management | ICT & Cybersecurity |
| LAU | Risk Management | |
| PDMFC | Introduction to Risk Management using Eramba or Simple Risk Open Source Software | Research and Development |
| PDMFC | ISO/IEC 27001 | Research and Development |
| FCT | Globalisation and Security Risks | NOVA Information Management Schools |
| MAG | Cyber Security Specialist | Maggioli Academy |
| MAG | Project Management | Maggioli Academy |
| Trustilio | Human Factors in Cybersecurity Management | |

To summarise, the CyberSecPro criteria Market Demand, Relevance to ECSF, and Course Availability are fulfilled. Accordingly, *Cybersecurity Risk Management* is included as Knowledge area for the CyberSecPro education and training programme.

Emerging Technologies

*Emerging Technologies* were mentioned 65 times in the survey with regards to important cybersecurity knowledge areas. Here again the high amount of mentions can be biased by a picture that was given in the survey as example for knowledge areas. The picture and some more detailed answers provide evidence that it was understood in the way that cybersecurity tools and solutions need to be developed to regulate *Emerging Technologies*. It cannot be directly associated to an ECSF job role. With regards to the CyberSecPro course portfolio there is not a particular course for cybersecurity for *Emerging Technologies*. However, the challenges around cybersecurity for *Emerging Technologies* are covered in many courses. Courses with a specific focus on *Emerging Technologies* will be treated under the umbrella of the Knowledge area of *Cybersecurity Tools and Technologies*. Therefore, cybersecurity for *Emerging Technologies* is not treated as independent Knowledge area in the context of CyberSecPro.

Cybersecurity Policy, Process, and Compliance

*Cybersecurity Regulations and Compliance* were mentioned as important Knowledge 58 times in the survey. Answers that were categorised in this knowledge areas are "Cybersecurity regulations/Cybersecurity compliance/Compliance". This Knowledge area directly relates to the ECSF job role of Cyber Legal, Policy & Compliance Officer. The person in this position manages the compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organisation's strategy and legal requirements. To accord for the terminology used within the ECSF, this Knowledge area will henceforward be referred to as *Cybersecurity Policy, Process, and Compliance.* The CyberSecPro consortium offers various courses related to this Knowledge area:

Table 8: CyberSecPro courses covering Cybersecurity Policy, Process and Compliance

| **Partner** | **Course** | **Department** |
|---|---|---|
| UPRC | Security Governance | Department of Informatics |
| UPRC | Security Policies and Security Management | Department of Digital Systems |
| UPRC | Operational Research | Department of Business Administration |
| UPRC | Information Security Governance, MSc | Department of Informatics |
| UPRC/FP/ Trustilio/ TUC | Cybersecurity Hands-On-Training (CyberHOT) | Joined series of seminars |
| UPRC | Cybersecurity Policies and Practices in the EU - for non-IT Experts | |
| LAU | Information Security Management | ICT & Cybersecurity |
| LAU | Risk Management | |
| PDMFC | Introduction to Risk Management using Eramba or Simple Risk Open Source Software | Research and Development |
| PDMFC | ISO/IEC 27001 | Research and Development |
| FCT | Globalisation and Security Risks | NOVA Information Management Schools |
| MAG | Cyber Security Specialist | Maggioli Academy |
| MAG | Project Management | Maggioli Academy |
| Trustilio | Human Factors in Cybersecurity Management | |

In conclusion, the CyberSecPro criteria Market Demand, Relevance to ECSF, and Course Availability are met. Therefore, *Cybersecurity Policy, Process and Compliance* will be covered within the CyberSecPro knowledge areas.

Cybersecurity Education and Training

In the survey, *Cybersecurity education and training* was mentioned by 49 respondents as important Knowledge area. It relates to the ECSF role of Cybersecurity Educator, who improves cybersecurity knowledge, skills and competencies of humans. In the context of the survey, it is, however, not always clear, how participants understood the term. Some participants included further thoughts on this Knowledge area, revealing that some meant that more training programmes for cybersecurity experts are needed, while others meant that more education and training in general (e.g. for all employees) is needed. Evidently, there cannot be a single course to satisfy the need for more training for cybersecurity experts. As a matter of fact, all courses within CyberSecPro aim to contribute to the satisfaction of this demand. The latter interpretation of *Cybersecurity education and training* sheds light on a different Knowledge area, namely *Human Factors* (see following section). Therefore, *Cybersecurity education and training* is not included as a Knowledge area in the context of CyberSecPro.

Cyber Incident Response

*Incident Response* was mentioned 49 times as important Knowledge area. It relates directly to the job of Cyber Incident Responder within the ECSF. A Cyber Incident Responder monitors the organisation's cybersecurity state, handles incidents during cyber-attacks and assures the continued operations of ICT systems. *Incident Response* (IR) is a reactive approach to dealing with attacks that have already happened. In contrast, Cybersecurity Threat Management (CTM) is a proactive approach to preventing attacks from happening. Both CTM and IR are essential for effective cybersecurity. The CyberSecPro consortium offers three courses dealing with *Incident Response*:

Table 9: CyberSecPro courses covering Incident Response

| **Partner** | **Course** | **Department** |
|---|---|---|
| LAU | Management of Cyber security | ICT & Cybersecurity |
| TalTech | Cyber Incident Handling | Department of Software Sciences, MSc |
| PDMFC | Incident Response & Network Intrusion Detection Systems | Research and Development |

In summary, *Incident Response* meets the three criteria Market Demand, Relevance to ECSF, and Course Availability. Consequently, it is added as a Knowledge area to the CyberSecPro education and training programme.

Network and Communications Security

In the survey, *Network and Communications Security* was mentioned 48 times as an important Knowledge area. Within the ECSF, it relates to the role of Cybersecurity Architect, who plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls. Several courses relating to this Knowledge area are offered by CyberSecPro consortium members:

Table 10: CyberSecPro courses covering Network and Communications Security

| **Partner** | **Course** | **Department** |
|---|---|---|
| UPRC | Network Security | Department of Informatics |

| | | |
|---|---|---|
| UPRC | Mobile and Wireless Communications Security | Department of Digital Systems |
| UPRC | Network Security | Hellenic Air Force Academy |
| UPRC | Network and Communications Security, MSc | Department of Informatics |
| LAU | Internet Infrastructure and Security | ICT & Cybersecurity |
| LAU | Network and Applications Security | ICT & Cybersecurity |
| UMA | Information Security | Computer Science |
| UMA | Design and Configuration of Secure Network Systems | Computer Science |
| UMA | Security in Industrial and Cyber-Physical Systems | Computer Science |
| FCT | Network and Computer Systems Security | Department of Informatics |

In summary, the CyberSecPro criteria Market Demand, Relevance to ECSF, and Course Availability are fulfilled. Accordingly, *Network and Communications Security* is included as Knowledge area for the CyberSecPro education and training programme.

### 2.3.2 Further Identified Topics

The fourth criterion for the selection of CyberSecPro knowledge areas is the importance to the effective protection of European cyber infrastructures and systems. The addition of this criterion introduces discussion topics that may have been inadequately addressed or overlooked in the survey conducted in the context of D2.3. knowledge areas in this section are derived from two sources: 1) free text answers from the survey that called for particular attention, and 2) discussions among CyberSecPro consortium members. By incorporating this qualitative step, we can introduce a valuable counterbalance to the earlier quantitative metrics, thereby addressing potential shortcomings in the survey. The inclusion of these knowledge areas opens up opportunities for considering important aspects that have been previously neglected or omitted in the analysis. In the following, their relevance and appropriateness for inclusion in the CyberSecPro education and training programme will be analysed.

Privacy and Data Protection

One topic that came into focus in the free text answers of the survey, was *Privacy and Data Protection*. However, there was a difference in the type of questions used for knowledge areas and cybersecurity skills. Participants were presented with a visual stimulus in the form of a picture depicting examples of knowledge areas (see Figure 3). but no such examples were provided for cybersecurity skills. Interestingly, Privacy and Data Protection were mentioned three times more frequently in the unbiased questions related to cybersecurity skills. As many of these answers for cybersecurity skills, mentioned *Privacy and Data Protection* on the first or second position, this finding stood out and let to the analysis of *Privacy and Data Protection* as a Knowledge area for the Cybersecurity education and training Programme.

The following quotes demonstrate the variety of *Privacy and Data Protection* dimensions that could be observed in the survey:

*"Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organisation"*

*"Explain and communicate data protection and privacy topics to stakeholders and users"*

*"Ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations"*

*"Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools"*

These aspects of *Privacy and Data* are all covered by the ECSF role of Cyber Legal, Policy & Compliance Officer, who shall (among other tasks) explain and communicate data protection and privacy topics to stakeholders and users and conduct, monitor and review privacy impact assessments. The CyberSecPro consortium offers the following courses covering *Privacy and Data:*

Table 11: CyberSecPro courses covering Privacy and Online Rights

| **Partner** | **Course** | **Department** |
|---|---|---|
| UPRC | Privacy on the Internet | Department of Digital Systems |
| UPRC | Security of Information and Network Systems - GDPR | Department of Informatics, MSc |
| PDMFC | GDPR | Research and Development |
| FCT | GDPR: Governance, Implementation, Maintenance and Control | NOVA Information Management Schools |
| UMA | Digital Identity and Privacy | Computer Science |
| UMA | Security and Privacy in Application Environments | Computer Science, MSc |

As the survey provides evidence for the market demand of *Privacy and Data*, the relevance to the ECSF framework is given, and the CyberSecPro consortium has courses available, it meets the criteria for a Knowledge area in the context of the CyberSecPro education and training programme. Due to the scope of the topic, it will be treated as independent Knowledge area, instead of incorporating it in *Cybersecurity Policy, Process, and Compliance.*

Human Factors in Cybersecurity

One topic that came up in different contexts of the CyberSecPro project were *Human Factors in Cybersecurity*. The following quotes that were taken from the D2.1 survey demonstrate some of the concepts of *Human Factors*:

*"In our (small-sized) business context, cybersecurity practical skills are needed especially on the basic level, most relevant to ensure secure use of digital services, and being well aware of the why and how"*

*"Acknowledging the fact the Cyb/Sec is NOT an IT matter, but a Company matter, require collaboration from all parties"*

*"This is not a training"-Mindset"*

In discussions among CyberSecPro consortium members, the following dimensions of *Human Factors* were identified:

I) Qualifying employees with regards to awareness and usage of cybersecurity tools

II) Building the organisation in a way that people can do cybersecurity. This involves ensuring that they are proficient in operating these tools and can integrate security tasks alongside their

primary responsibilities without compromising their productivity or straying from their designated job roles

III) Building cybersecurity tools with people in mind. Humans are often the weakest link in the security chain. A user-friendly and intuitive interface increases the likelihood of individuals correctly configuring and utilising security tools, reducing the risk of accidental breaches or system vulnerabilities caused by human error. Moreover, by enhancing the user experience of cybersecurity tools, there is a higher probability of their widespread adoption and usage.

These dimensions can also be found in the ECSF job roles: 1) A Cybersecurity Educator shall design, develop and conduct awareness, training and educational programmes in cybersecurity and data protection-related topics, 2) a Chief Information Security Officer shall influence an organisation's cybersecurity culture, and 3) a Cybersecurity Architect shall propose cybersecurity architectures based on stakeholder's needs and budget and collaborate with other teams and colleagues. Some of the topics discussed here are related to *Cybersecurity education and training*. However, entitling the Knowledge area *Human Aspects in Cybersecurity* allows a more well-rounded and comprehensive approach. Currently, the CyberSecPro Consortium offers only one course specifically dedicated to *Human Aspects in Cybersecurity:*

Table 12: CyberSecPro courses covering Human Factors

| **Partner** | **Course** | **Department** |
|---|---|---|
| Trustilio | Human Factors in Cybersecurity Management | |

Nevertheless, other partners such as TalTech have course material available to generate new courses both on undergraduate and graduate level. Therefore, to account for the importance of this aspect, *Human Aspects in Cybersecurity* are included in the list of knowledge areas.

Soft Skills for Cybersecurity

Several answers in the D2.1 survey regarding *Soft Skills for Cybersecurity* stood out. In the following some exemplary quotes are presented:

*"Broad creative thinking skills"*

*"Information warfare: disinformation, misinformation and fake news security"*

*"Inter-disciplinary interaction, communication, collaboration"*

*"Ability to discuss about this area with customers"*

*"Communication skills in business language"*

These excerpts illustrate three topics that can be observed: 1) Critical and creative thinking, 2) collaboration, and 3) communication skills. These *Soft Skills for Cybersecurity* did not reach the required threshold of more than 40 mentions nor can they be linked to an ECSF job role. Nevertheless, they seem critical in the development of a sustainable cybersecurity infrastructure for the future, as will be discussed in the following:

As we rely more on technology for communication, problem-solving, and decision-making, developing critical thinking becomes an essential skill to protect individual autonomy and develop innovative cybersecurity solutions. In this context, diversity should be added as additional prerequisite to developing a sustainable cybersecurity infrastructure. By incorporating individuals with diverse backgrounds, genders, races, ethnicities, and cultures, different ways of thinking and problem-solving can be fostered, leading to innovative strategies and solutions. An inclusive and diverse cybersecurity workforce promotes a stronger defence against emerging threats and cyber-attacks. Hackers often exploit weaknesses in systems that have not been adequately tested by a diverse group, and having a heterogeneous team can help anticipate and mitigate potential risks. Furthermore, inclusion promotes fairness and equality in the industry, offering opportunities for underrepresented groups to contribute

their skills and expertise. By embracing diversity, the cybersecurity field can bridge the existing gender and racial gaps, creating a more equitable and just professional environment.

Collaboration is another key aspect emphasised here. Cybersecurity is not solely an individual effort; it necessitates a collective endeavour involving professionals from various domains such as technology, policy, and law enforcement. Collaboration enables users to share knowledge, experience, and expertise to create a comprehensive and holistic cybersecurity infrastructure. By working together, professionals can pool their diverse perspectives and skills, strengthening their collective defences against cyber threats.

The importance of communication skills is also highlighted. Its significance cannot be overstated in the field of cybersecurity. It is crucial for cybersecurity professionals to communicate complex technical concepts in a clear and understandable manner to non-technical individuals such as employees, executives, customers, and policymakers. This communication is essential in conveying the importance of cybersecurity and fostering a culture where everyone is aligned and educated on its significance. By mastering effective communication, cybersecurity professionals can establish trust and credibility with non-technical stakeholders. Additionally, they can develop the ability to actively listen, understand the concerns of stakeholders, and address them appropriately.

Overall, critical and creative thinking, collaboration, and communication skills seem to be fundamental pillars in developing a robust cybersecurity infrastructure. By fostering these skills, organisations and individuals can better anticipate, counter, and mitigate cyber threats, ensuring the data security and privacy. Among the members of the CyberSecPro Consortium, no course covers these *Soft Skills for Cybersecurity* in particular. Therefore, the topics will be incorporated in the knowledge areas *Cybersecurity Management* and *Human Aspects in Cybersecurity*.

## 2.4 Detailed Knowledge Areas

### 2.4.1 Penetration Testing

Penetration testing, also known as ethical hacking, is a critical cybersecurity practice that involves legally hacking into organisations' computer systems, networks, and software applications to uncover vulnerabilities and weaknesses. During penetration testing (black box or white box), real-world cyber-attacks are simulated to evaluate the security of organisations' systems to provide actionable intelligence that helps improve system defences. Penetration testing is also considered a proactive practice an organisation relies on to identify systems' potential entry points for cyber-attacks and re-enforce security. There are various types of penetration testing that target different parts of an organisation's overall IT infrastructure, including network, web applications, mobile, IoT (Internet of Things), and cloud penetration testing. Each type focuses on assessing and identifying vulnerabilities in different areas of technology and infrastructure.

The lifecycle of a penetration test consists of several stages, including engagement, information gathering, foot printing and scanning, vulnerability assessment, exploitation, and reporting. The engagement phase involves establishing agreements and policies between the tester and the organisation. Information-gathering entails collecting data and intelligence for later use. Footprinting and scanning refer to examining the architecture and entry points of the target system. Vulnerability assessment focuses on identifying weaknesses and assessing their risk level. The exploitation phase involves attempting to exploit the vulnerabilities to gain unauthorised access. Finally, the reporting phase includes providing a detailed report with findings, proof of concepts, and recommendations for mitigating the identified issues.

Penetration testing is pivotal in empowering businesses to uncover vulnerabilities and weaknesses within their systems ahead of malicious actors who could exploit them. Consistently incorporating comprehensive penetration testing is essential for remaining ahead of potential threats and ensuring the utmost security of sensitive data while ensuring business continuity. Furthermore, penetration testing is indispensable to upholding robust security measures for systems and infrastructure in today's digital world. By proactively identifying vulnerabilities and weaknesses via meticulous penetration testing,

organisations can implement targeted measures to mitigate risks and protect sensitive data. Adhering to the established lifecycle of a penetration test and leveraging specialised testers across various domains empowers businesses to bolster their security posture, adeptly outmanoeuvring potential threats.

However, penetration testing is usually performed by skilled cybersecurity professionals, who may be internal or external to an organisation. Recent studies [1] [2] [3] [4] [5] have shown that the cybersecurity labour market is experiencing a shortage of qualified professionals for various cybersecurity positions, including Penetration Testers. In this regard, several cybersecurity workforce development skills frameworks have identified penetration testing as an essential Knowledge area that training programmes should also consider. Moreover, CyberSecPro's state-of-the-art analyses of cybersecurity market demand and supply, coupled with the outcome of a survey [1], revealed that penetration testing is one of the critical knowledge areas that should be included in the CyberSecPro curriculum owing to its high demand.

### 2.4.2 Cybersecurity Tools and Technologies

CyberSecPro's recent study [1] emphasised the relevance of cybersecurity tools and technologies in securing and protecting individual and organisation's ICT infrastructure. The study further underscored that cybersecurity tools and technologies are critical in implementing effective and efficient defensive and protective measures that safeguard the organisation's vital data ICT assets. The report also indicated a high demand for cybersecurity professionals skilled in cybersecurity tools and technologies, hence its consideration in the CyberSecPro curriculum.

The increasing volume of digital assets and the complex, digitally interconnected world make cybersecurity a primary component to be considered by individuals and organisations to remain safe and in business. There is also a corresponding increase in the frequency of cyberattacks and the sophistication of such attacks, giving rise to an array of cybersecurity tools and technologies that enable individuals and organisations to protect their digital assets and data while ensuring business continuity.

At the basic level of protection are cybersecurity tools such as antivirus software. This software performs routine scans of files and applications to detect and deal with malicious code and other suspicious activities within an individual or organisation's software or information systems. Above antivirus software are network firewalls, an essential cybersecurity technology. Firewalls protect ICT infrastructure as a barrier between an organisation's trusted network and external networks. Firewalls may be implemented at the hardware or software levels to prevent unauthorised access and data exfiltration. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) constitute another category of essential cybersecurity tools that identify and respond to potential cyber-attacks. Other essential tools and technologies include endpoint security platforms, encryption, security information and event management (SIEM) tools such as Splunk and IBM QRadar.

Furthermore, emerging technologies such as AI, Machine Learning, and IoT have created new opportunities for cyber attackers to exploit organisation's ICT infrastructure; thus, safeguarding these technologies from cyber threats remains a priority. These technologies' inherent characteristics and capabilities make them potential targets for cybercriminals. For instance, the data exchange capabilities of IoT devices could be prone to cyber-attacks. Ensuring cybersecurity for emerging technologies like AI, Machine Learning, and IoT is complex and necessary, making it essential for cybersecurity training programmes to consider them in their offering so upcoming experts can understand these technologies and how they can be protected against cyber threats. Cybersecurity defence measures must also evolve as these technologies evolve rapidly to counter existing and emerging threats. A skilled cybersecurity professional workforce can implement robust cybersecurity strategies and promote user awareness towards effectively protecting these innovative technologies from cyber threats.

Given the vast array of cybersecurity tools and technologies that are continuously emerging and available to organisations, a professional cybersecurity training curriculum should consider these tools and technologies, especially hands-on training that equips trainees with the proper knowledge to join the army of cybersecurity professionals currently in short supply.

### 2.4.3 Cybersecurity Management

Cybersecurity management (CM) involves the overall management of an organisation's cybersecurity strategy and its implementation to ensure its network, information systems, and other assets are effectively secure and protected. Cybersecurity management is considered a crucial aspect of organisations that have embraced digital transformation. The consequence of digital transformation is that more organisations become interconnected, and the digital ecosystem increases complexity and associated cyber threats. CM entails planning, implementing, and monitoring defensive mechanisms to secure and protect the organisation's data and IT infrastructure against all forms of malicious cyber threats and attacks.

Successful cybersecurity management is fundamental to securing and protecting an organisation's data and winning client trust while ensuring business continuity. Since CM adopts both proactive and reactionary approaches to cybersecurity, organisations need to provide the proper awareness and training of its employees, especially the Chief Information Security Officer (CISO) (also known as information security officer, information security manager, head of information security, IT/ICT security officer) whose role is primarily to oversee the organisation's cybersecurity strategy and policy. A CISO maintains and communicates the organisation's vision, strategy, policies, and processes. A CISO also oversees the implementation of the cybersecurity policy across the organisation and manages information interchange among professional agencies and government authorities [6]

As the head of an organisation's cybersecurity strategy and policy, a CISO is saddled with enormous responsibilities well-defined by several cybersecurity workforce development frameworks, including ECSF.The ECSF clearly outlined several tasks a CISO performs and the skills, knowledge, and competencies the CISO needs to discharge his role effectively and efficiently. Recent research and reports [1] [7] [8] have shown that the number of qualified cybersecurity professionals who can take up CISO roles are grossly inadequate. The high demand for CISO makes it imperative for CyberSecPro to include CM as a Knowledge area in its cybersecurity training offering. It is also expected that the CyberSecPro consortium and HEIs across the EU would further enhance their curricula to emphasise practical cybersecurity hands-on training that would equip trainees to undertake CISO roles and meet cybersecurity labour market needs.

### 2.4.4 Cybersecurity Threat Management

In an increasingly complex and digitally interconnected world, cybersecurity threat management (CTM) is another critical aspect that organisations must deal with to safeguard their data and critical IT infrastructure. CTM offers a holistic approach to identifying, assessing, mitigating, and monitoring cyber threats. CTM follows a proactive approach in combating cyber threats. Because cyber threats are always evolving and pervasive, a proactive approach is justified, as organisations remain ahead of malicious threats, minimising threat impact while keeping the business afloat.

One of the key aspects of CTM is threat identification, which is often undertaken by a Cyber Threat Intelligence Specialist (CTIS) who gathers, processes, and analyses data and information to produce actionable intelligence. Therefore, threat intelligence primarily involves identifying potential threats and vulnerabilities that could compromise an organisation's network, data, and information systems.

However, within ECSF, CTM includes digital forensics, a role undertaken by a Digital Forensic Investigator (DFI). Cyber forensics primarily focuses on recovering, analysing, and preserving digital evidence for legal proceedings. The goal is to identify criminals, uncover their methods of operation, and contribute to the prevention of future criminal activities. Cyber forensics encompasses various specialised areas, including computer forensics, mobile device forensics, and network forensics, each dedicated to examining specific types of digital evidence. Closely related to CTIS, a DFI's primary objective is to methodically collect, analyse, and safeguard evidence that can shape investigations.

Cyber threat intelligence and cyber forensics have their share of challenges, thus requiring professionals to be highly skilled in both fields of work. Extracting data from locked or damaged devices, grappling with voluminous amounts of data, ensuring the integrity of the acquired evidence, and meticulously preserving the digital chain of custody pose formidable obstacles that a skilled professional can overcome. Under the umbrella of CTM, CTIS and DFI enable a comprehensive analysis of digital evidence, facilitating the identification of criminals, recovering deleted data, and generating exhaustive investigative reports.

CTM has significant relevance in the business realm, especially in ensuring business continuity, particularly within incident response processes. Owing to the significance of CTM, several frameworks and standards [9] [10] [11] have been established to help organisations manage threats. Cyber forensic investigators assume pivotal roles in investigating security breaches, meticulously analysing the pathways employed by perpetrators, and meticulously recovering data from compromised devices. At the same time, their threat intelligence counterpart takes proactive measures that help to protect and secure the organisation's IT infrastructure. An in-depth understanding of the historical background, distinct phases, and cutting-edge tools employed in cyber threat intelligence and forensics empowers professionals in this dynamic field.

Given CTM's multifaceted and dynamic nature, there is a growing demand for skilled cybersecurity professionals knowledgeable in threat intelligence and forensics to deploy a combination of technical solutions that leverage risk assessment, incident response capabilities and human factors. In this vein, CyberSecPro considers CTM an essential Knowledge area that should be included in its curriculum.

### 2.4.5 Risk Management

Risk management has continued to be a critical Knowledge area within the cybersecurity ecosystem. It has also proven to be an essential cybersecurity Knowledge area that cybersecurity professionals, especially upcoming experts, must include in their professional capacity development portfolio. The importance of cybersecurity risk management knowledge for the future cybersecurity professional cannot be overemphasised, even as it remains a prominent crucial domain in the European Cyber Security Body of Knowledge (CyBOK) [12].

According to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), risk management involves activities ranging from *"overseeing, evaluates, and supports documentation [sic.], validation, assessment, and authorisation processes necessary to assure that existing and new information technology (IT) systems meet the organisation's cybersecurity and risk requirements"* [13]. It further opines that a cybersecurity risk management initiative ensures risk treatment, compliance, and assurance based on internal and external viewpoints. In its latest version, the European Cybersecurity Skills Framework (ECSF) also considered the relevance of cybersecurity risk management by designating the profile of a Risk Manager who oversees risk management and governance within an organisation. Both NIST CSF and ECSF provide several characteristics of a risk manager, including abilities, sub-knowledge areas, skills, and task and capability indicators. The CyberSecPro professional training programme seeks to train risk managers who embody these characteristics to benefit the EU cybersecurity labour market.

As a Knowledge area, risk management has been repeatedly considered in several cybersecurity workforce development initiatives, including frameworks, strategies and guidelines. The renowned NIST CSF framework in all its versions considers risk management a speciality area vital to cybersecurity workforce development. Similar cybersecurity frameworks (e.g. Saudi Arabian cybersecurity framework, Czech cybersecurity framework, Australian Cybersecurity Framework, among others) that have been inspired by NIST CSF have also maintained risk management as a key cybersecurity domain knowledge cyber experts should acquire. A recent cybersecurity professional market analysis study [1]. found that risk management remains one of the highly demanded knowledge areas and skills the market requires of cybersecurity professionals. This outcome justifies the inclusion of risk management as a key Knowledge area in the existing cybersecurity skills framework. It also explains its inclusion in the CyberSecPro professional training programme.

### 2.4.6 Cybersecurity Policy, Process and Compliance

As private and public organisations continuously embrace digital transformation, the global communication and network infrastructure increases with a corresponding rise in interconnected devices and services. As a result, more data and organisations' critical infrastructure are available online, thus open to various malicious cyber-attacks and threats. For governments and organisations to thrive and successfully function in the face of current and emerging cyber-attacks and evolving threats against their cyber-physical infrastructure, they must develop, adopt, and implement policies, standards and certifications for the cybersecurity ecosystem.

Cybersecurity policies prescribe high-level business rules and principles that govern how an organisation intends to protect and defend its communication and network infrastructure, including the databases and applications that run on the infrastructure. At an organisational level, a typical cybersecurity policy identifies the technologies and information assets that need protection, threats to the assets, rules and controls governing the protection of the assets and business in general. Cybersecurity standards [14], on the other hand, provide the granular requirement for operationalising a cybersecurity policy. In a broader sense, cybersecurity standards are often provided by approved external bodies, including government and private agencies. For instance, the European Union Agency for Cybersecurity (ENISA) establishes policies and standards that govern cybersecurity across the EU. The International Organisation for Standardisation (ISO) is widely known for providing standards. Standardisation of digital communications and other related products and services that impact cybersecurity is necessary to ensure consistency and create trust among all stakeholders, especially manufacturers, developers and clients. ENISA aims to realise cybersecurity cohesion and harmonisation and provide support that enables a single European digital market for cybersecurity while securing critical elements across the cybersecurity landscape [15].

However, in contrast to policies and standards, cybersecurity certifications are schemes designed to facilitate a formal evaluation of cybersecurity products, services, and all related processes. An approved or accredited agency often performs certification based on a well-defined set of criteria. A successful evaluation exercise may lead to issuing a certificate to demonstrate compliance. The EU's Cybersecurity Act provides a cybersecurity certification framework with the primary aim of developing certification schemes that enable the assessment and certification of products, services, and processes [15].

Furthermore, cybersecurity compliance involves individuals and organisations complying with established policies, standards, and regulations that protect individuals' and organisations' network and computer systems, software applications and data against cyber threats. In the EU, some of the policies, regulations and frameworks organisations and members of the public are required to comply with are enshrined in the European General Data Protection Regulation (GDPR), the Network and Information System Directive and the EU Cybersecurity Act. Cybersecurity compliance is fundamental to cyber risk mitigation and fosters trust among individuals, business organisations and regulatory agencies.

Current and next-generation cybersecurity professionals should be knowledgeable about existing cybersecurity policies, standards, relevant certifications, and compliance and how they impact their work. It is also essential for cybersecurity professional training programmes to include policies, standards, and certifications as a key Knowledge area to enable new professionals to achieve the know-how of developing new policies, standards, and certifications at the various levels required of their working roles.

### 2.4.7 Incident Response

Safeguarding computer systems and networks from threats is paramount, making cyber security operations and incident response crucial. These coordinated operations encompass proactive monitoring, detection, and effective mitigation of security incidents like malware attacks, data breaches, and unauthorised access attempts. Incident response entails a systematic approach to promptly address security incidents, minimising harm and restoring normal operations. Swift containment, meticulous investigation, complete eradication, and seamless recovery are critical components of a cyber incident response. The expertise of skilled professionals, adept at analysing security logs, deploying protective

measures, and collaborating with stakeholders, ensures an agile and efficient response. By upholding information systems' integrity, confidentiality, and availability, cyber security operations and incident response prevent disruptions to critical business processes and safeguard sensitive data.

An organisation's incident response management requires an incident response plan, a set of coordinated instructions to assist detection, response, and recovery from cyber security incidents. A well-developed incident response plan provides a straightforward course of action for dealing with cyber incidents, which may result in massive network or data breaches that may impact an organisation. Following the plan, an organisation can quickly stop, contain, and control the cyber incident. A separate disaster recovery plan is created for physical disruptions like natural disasters or flooding. An organisation's cyber incident recovery team is usually responsible for implementing the incident response plan. Typically, this team consists of IT staff members whose roles include collecting, preserving, and analysing incident-related data. Depending on the situation, they may also collaborate with legal professionals and communications experts to ensure compliance with legal requirements.

The need for an incident response plan arises from the inevitability of cyber threats as more organisations and individuals make their IT infrastructure available online. Whether a network has already faced a cyber-attack or not, the chaos that ensues could be disastrous. Cyber threats, including network and data breaches and physical threats, such as power outages or natural disasters, can result in data or functionality losses that severely affect an organisation. An incident response plan, along with a disaster recovery plan, helps mitigate risks and prepares for a range of events. Therefore, to deal with cyber incidents and ensure business continuity, organisations must have a well-defined incident response plan and a skilled professional cybersecurity incident response team to execute the plan successfully. Existing research has shown that the cybersecurity labour market has inadequately qualified professionals in cyber incident response handling. Our previous study also showed that incident response is a highly demanded Knowledge area in the cybersecurity labour market and, therefore, included in the CyberSecPro training curriculum.

### 2.4.8 Network and Communication Security

Internet's ubiquity remains an enabler for the interconnectivity of millions of devices to the network. These interconnected devices have access to several software applications and services owned or offered by private and public organisations. Organisations and their business have, therefore, perpetually relied on networked communication technologies to function effectively.

Communication and network security involve undertaking operations to protect and defend organisations' networked communication systems (including databases and software applications). From the standpoint of the CIA triad model [16], the goal of providing protection and defence would be to ensure the confidentiality, integrity and authentication of communication systems in addition to non-repudiation of users and information management. Due to businesses' continuous dependence on network communications systems and their susceptibility to cybersecurity attacks, it is necessary to incorporate communication and network security technologies to ensure business continuity further.

Protecting and defending networked communication systems and ensuring business continuity is an enormous responsibility that stakeholders, especially cybersecurity professionals, must shoulder daily. They must therefore be vested in communication and network security knowledge to succeed in this role. Existing cybersecurity workforce skills development frameworks have identified communication and network security as a fundamental Knowledge area that must be included in any cybersecurity professional training programme. It is also one of the knowledge areas in the European cybersecurity body of knowledge. A recent cybersecurity labour market analysis reported in [1] also found that the labour market needs cybersecurity professionals with proven communication and network security knowledge. The report indicated that communication and network security is a Knowledge area in high demand. The NIST CSF, Czech and other similar frameworks comprehensively defined the industry role of a network operations specialist in terms of abilities, skills, knowledge, tasks and capability indicators.

### 2.4.9 Privacy and Data Protection

As more private and public organisations continue to embrace digital transformation, more organisations' data become available and exposed to cyber threats. Digital transformative initiatives are not without concerns, as stakeholders highlight privacy concerns that must be addressed by organisations desiring to go digital, especially cloud-based digital solutions. Therefore, data protection and privacy-affirming technologies must support a digital transformation initiative to gain stakeholders' trust while ensuring business continuity.

Furthermore, since data protection and privacy technologies play a crucial role in safeguarding sensitive information and ensuring compliance with privacy regulations, organisations must use these technologies to their advantage. Data protection and privacy technologies embody a range of tools, platforms, technologies, and strategies for protecting data and ensuring privacy. Some essential aspects of data protection and privacy technologies include data loss prevention, encryption, access controls, privacy-enhancing technologies, data anonymisation and pseudonymisation.

In response to current and emerging cyber-attacks and threats against data and privacy, organisations must adopt these technologies to enhance data protection and privacy. The European cybersecurity labour market needs an army of professionals knowledgeable in data protection and privacy technologies to protect and defend organisations' infrastructure and businesses against growing cyber-attacks and threats.

### 2.4.10 Human Aspects of Cybersecurity

Another Knowledge area that is critical to securing and protecting an organisation's ICT infrastructure is the human aspects of cybersecurity. CyberSecPro's recent study [1] has shown that an organisation's cybersecurity defensive measures are incomplete without considering the human elements of cybersecurity, even as cyber-attacks and threats continue to evolve. Human aspects of cybersecurity also referred to as human factors, deal with human behaviour, awareness, and cybersecurity education of cybersecurity professionals and every employee of an organisation. These human aspects have the potential to weaken or strengthen cyber defences depending on how organisations leverage these factors.

Phishing attacks and social engineering can be viewed from the lens of human aspects of cybersecurity as attackers exploit identified human vulnerabilities. Through these attacks, a would-be attacker deploys psychological tactics to manipulate unsuspecting individuals to reveal sensitive information that allows them to cease control and gain unauthorised access to the organisation's network, data, and information systems. Insider threats involving staff and other trusted individuals, such as external consultants, can compromise the organisation's cybersecurity defences via their deliberate misuse of access. Security awareness training, cultural and organisational factors, and user-centric security are essential approaches within the umbrella of human aspects of cybersecurity that organisations can employ to train employees on cybersecurity best practices and acknowledge "people" as the organisation's cybersecurity first line of defence.

The ECSF job roles of Cybersecurity Educator (CE), CISO, and Cybersecurity Architect (CA) underscore the need for organisations to consider human aspects of cybersecurity. This need is also highlighted in a recent study [1] conducted within CyberSecPro. For instance, a CE designs, develops, and conducts awareness training and educational programmes in cybersecurity and other topics related to data protection. A CISO, on the other hand, influences the organisation's cybersecurity culture by implementing an established cybersecurity strategy and policy that are reviewed from time to time to combat existing and emerging cyber threats. On the other hand, the CA drafts cybersecurity architectures that are informed by stakeholders while collaborating with other teams within and outside the organisation. Owing to the significance of human aspects of cybersecurity, cybersecurity professional training curricula need to consider human factors as an essential Knowledge area that trainees must be skilled in, hence its inclusion in the CyberSecPro curriculum.

## 2.5 Summary and Discussion

This chapter has contributed an analysis and selection of Cybersecurity knowledge areas in the context of the CyberSecPro education and training programme. The selection criteria have been 1) market demand, 2) relevance to the ECSF, 3) availability of resources, and 4) importance. The analysis resulted in ten knowledge areas. Their importance is backed by an extensive and comprehensive review of existing literature and best practices in cybersecurity education and research across and beyond the EU cybersecurity landscape. It is important to note that previous CyberSecPro studies [1] specifically mapped and analysed cybersecurity knowledge areas and skills offered across EU HEIs programmes with those needed in the labour market to establish knowledge and skills gaps – the result of which strongly support the selected knowledge areas presented in this report. Also included in the analyses are the outcomes of cybersecurity workforce development initiatives undertaken by ENISA and notable EU-funded projects such as REWIRE, CONCORDIA, ECHO, ECSO, ESCO and SPARTA. The following list summarises the key concepts and skills in each selected knowledge areas for the CyberSecPro education and training programme (in descending order of mentions in the market demand survey):

1. **Penetration Testing:** Penetration testers simulate cyberattacks to identify system, network, or application vulnerabilities. They use various tools and techniques, including vulnerability scanners, password-cracking tools, and social engineering tactics.
2. **Cybersecurity Tools and Technologies:** Cybersecurity professionals must be familiar with a wide range of tools and technologies designed to protect against cyberattacks. These tools include firewalls, intrusion detection systems, antivirus software, and other advanced solutions.
3. **Cybersecurity Management:** Cybersecurity managers develop and enforce security policies and procedures, oversee cybersecurity tool deployment, and manage the financial aspects of cybersecurity initiatives.
4. **Cybersecurity Threat Management:** Cybersecurity threat management professionals monitor the threat landscape, identify new threats, and formulate mitigation strategies.
5. **Cybersecurity Risk Management:** Cybersecurity risk management experts identify, assess, and manage cybersecurity risks. They identify vulnerable assets, evaluate the likelihood and impact of potential threats, and develop strategies to mitigate these risks.
6. **Cybersecurity Policy, Process, and Compliance:** Cybersecurity policy, process, and compliance professionals develop and enforce security policies and procedures. They also ensure organisations comply with relevant regulations, conduct security audits, and manage risk assessments.
7. **Cyber Incident Response:** Incident responders contain attacks, eliminate threats, and restore affected systems to normal operation.
8. **Network and Communications Security:** Network and communications security professionals design and implement secure network architectures, configure network devices, and monitor network traffic for anomalies.
9. **Privacy and Data Protection:** Privacy and data protection experts develop and enforce privacy policies and procedures, manage data access, and respond to data breaches.
10. **Human Aspects of Cybersecurity:** Human aspects of cybersecurity professionals educate and engage employees in cybersecurity practices.

Each of the CyberSecPro knowledge areas is essential for cybersecurity professionals, as they collectively provide a well-rounded understanding of cybersecurity. In today's cyber landscape, where threats are diverse and ever-changing, professionals must possess multifaceted skills and knowledge to protect organizations effectively.

- Penetration testing and cybersecurity tools are essential for identifying vulnerabilities and deploying the right defences.
- Cybersecurity management and risk management ensure that organizations have a strategic and cost-effective approach to security.

- Threat management and incident response are critical for detecting and mitigating attacks swiftly.
- Privacy and data protection are paramount for maintaining trust and complying with privacy regulations.
- Network and communications security are crucial to prevent attacks from infiltrating the infrastructure.
- The human aspects of cybersecurity underscore the need to create a security-conscious workforce.

In summary, the CyberSecPro knowledge areas provide a comprehensive roadmap for cybersecurity professionals, encompassing the field's technical, managerial, and human aspects. In a constantly evolving threat landscape, these knowledge areas serve as a guide to safeguard organizations from cyberattacks, emphasizing the importance of a holistic approach to cybersecurity. Cybersecurity professionals who master these areas will be well-prepared to address the challenges and threats of the modern digital age.

### 2.5.1 Interrelations between Knowledge Areas

Notably, the scope of these knowledge areas is quite diverse. However, this variation is not an issue, but rather reflects the real need of the market due to the varying maturity levels and needs of organisations and individuals. There are several reasons why this variation is beneficial:

1. By providing both broad and specific knowledge areas, the programme enables learners to specialise in a particular domain of interest.
2. By having knowledge areas that vary in scope, the programme can evolve over time to incorporate the latest developments in the industry. This ensures that the programme remains relevant and meets the demands of the market.
3. Organisations and individuals have different levels of cybersecurity maturity. Some may be at the beginner stage, requiring foundational knowledge, while others may be more advanced, seeking specialised insights. By offering both broad and specific knowledge areas, the programme can cater to the varying maturity levels, enabling learners to choose the appropriate level of education that aligns with their current needs and skillset.

Figure 5 provides an overview of the CyberSecPro Knowledge area and their relation to each other. Three knowledge areas build the basis: 1) *Cybersecurity Policy, Process, and Compliance,* 2) *Cybersecurity Management,* and 3) *Tools and Technology*. *Cybersecurity Policy, Process, and* Compliance involves the development and implementation of cybersecurity policies and processes to ensure compliance with relevant laws and regulations. It is interconnected with *Cybersecurity Management* as it provides the guidance and framework for managing cybersecurity within an organisation. *Cybersecurity Management* involves the overall management and governance of the cybersecurity programme within an organisation. It is closely interconnected with various other knowledge areas, i.e. *Cybersecurity Policy, Process, and Compliance*, *Cybersecurity Risk Management*, *Cybersecurity Threat Management*, and *Incident Response*. *Tools and Technologies* is an abstract category dealing with the tools, software, and hardware used to secure systems. Hence, it relates to *Penetration Testing* and *Network and Communication Security* as these tools play a crucial role in monitoring and securing networks.

Next, we have four knowledge areas that are closely interrelated: 1) *Cyber Incident Response*, 2) *Cybersecurity Threat Management*, 3) *Cybersecurity Risk Management*, and 4) *Penetration Testing. Cybersecurity Threat Management* is a proactive approach to preventing attacks from happening, while *Incident Response* is a reactive approach to dealing with attacks that have already happened. *Cybersecurity Threat Management* is also closely related to *Cybersecurity Risk Management.* This Knowledge area is concerned with identifying, assessing, and managing risks in relation to cybersecurity. It encompasses evaluating the potential impact and likelihood of threats, vulnerabilities, and attacks. Both *Cybersecurity Risk Management* and *Cybersecurity Threat Management* are

interconnected with *Penetration Testing.* This Knowledge area involves simulating attacks on a system to identify vulnerabilities and weaknesses.

Finally, there are two overarching knowledge areas that influence all other knowledge areas: 1) *Privacy and Data Protection,* and 2) *Human Aspects of Cybersecurity*. *Privacy and Data Protection* involves the protection of sensitive information and personal data from unauthorised access, use, or disclosure. It is interconnected with all other knowledge areas as privacy and data protection considerations need to be integrated into all aspects of cybersecurity practices. *Human Aspects of Cybersecurity* recognises the importance of human behaviour, awareness, and training in maintaining cybersecurity. It influences all other knowledge areas as human actions can significantly impact the effectiveness of cybersecurity measures and response.

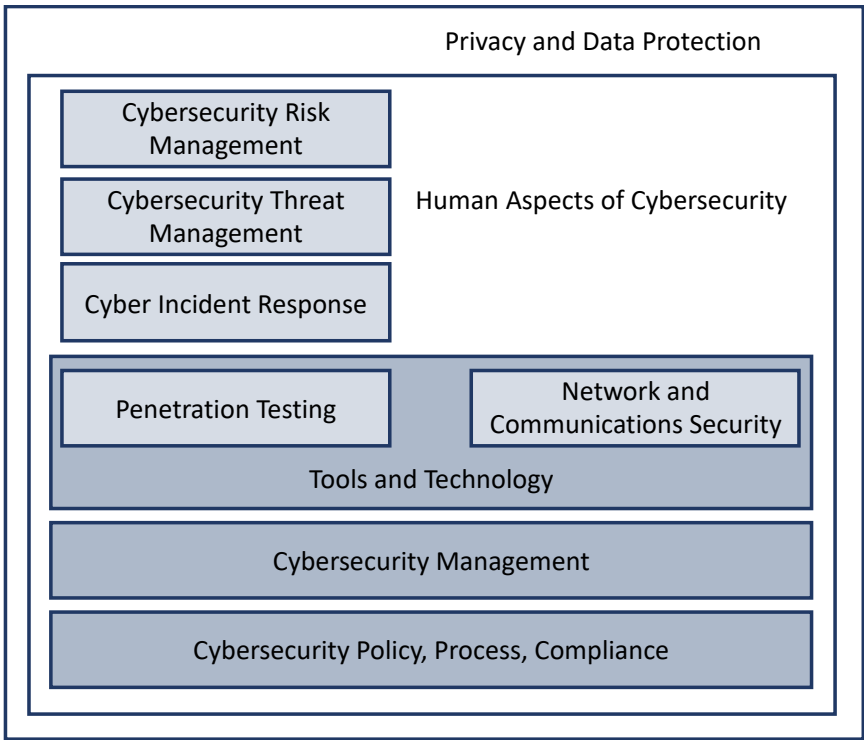



Figure 4: Overview of CyberSecPro knowledge areas

### 2.5.2 Derivation of Training Modules

One limitation in the selection process of knowledge areas is the reliance on the main clusters of courses identified in D2.2. Even though a more detailed analysis would yield higher accuracy, the advantage of time and resources saved in not having to evaluate each course for every possible Knowledge area individually outweighs the necessity for such detailed analysis in this specific context. However, as a result the list of courses within the knowledge areas might not be entirely representative. To account for this shortcoming the next chapter on education and training modules will conduct the analysis backwards and map the courses to the final selection of knowledge areas.

### 2.5.3 Sector Specific Knowledge Areas

It is important to understand that while the survey received a significant number of responses, it is not necessarily representative. As a consequence of the limited size of the sample, it is not possible to draw a reliable conclusion regarding the specific priorities in each sector from the survey. However, the state-of-the-art analysis and survey conducted in D.2.1 have revealed that the selected CyberSecPro knowledge areas are in high demand across all sectors, including health, maritime, and energy. In line

with this, CyberSecPro aims to enhance its training offerings by customising the content to cater to the specific needs of these sectors. Through the implementation of sector-specific scenarios, exercises, and test cases, the training material in the areas of maritime, energy, and health will be tailored to meet the requirements of stakeholders

# 3 CyberSecPro Education and Training Modules

## 3.1 Introducing Education and Training Modules

CyberSecPro aims to offer state-of-the-art cybersecurity education and training modules considering market demand and CyberSecPro partners' supply of cybersecurity training offerings. CyberSecPro's approach addresses the gaps in the European cybersecurity workforce and consolidates EU cybersecurity posture and competitiveness. Previously, chapter 3 provided a comprehensive analysis of cybersecurity knowledge areas in order to prioritise knowledge areas that target cybersecurity workforce skills demands and are fulfilled by CyberSecPro partners' cybersecurity education and training programmes. The Knowledge area analysis resulted in ten knowledge areas passing the pre-established criteria for inclusion in the CyberSecPro professional training curriculum. This chapter focuses on selecting cybersecurity education and training modules that align with the prioritised knowledge areas. Consortium members will further develop, enhance, and supply these education and training modules. CyberSecPro partners may deliver education and training modules in various forms, including seminars, courses, workshops, summer schools, hackathons, MOOCs and other suitable formats.

The CyberSecPro training modules cover most of the European cybersecurity market demanded workforce knowledge, skills, and competencies. It is important to note that some of the most sought-after cybersecurity recruitment or job specification buzzwords are not adapted in the CyberSecPro education and training module naming conventions. However, the content is provided within the CyberSecPro training module syllabus. For example, cybersecurity for emerging technology, artificial intelligence and cybersecurity tools and technologies are already covered in CyberSecPro training module syllabus within selected CyberSecPro modules.

## 3.2 Methodology of Selection

The CyberSecPro education and training programme aims to bridge the gaps in cybersecurity workforce skills development by carefully selecting knowledge areas and corresponding education and training modules. The selection process for the education and training modules ensures that the programme covers all the necessary skills and knowledge required in the field.

To select the appropriate education and training modules, all course offerings provided by CyberSecPro partners are carefully reviewed. Each course is thoroughly evaluated and mapped against the ten selected knowledge areas. This mapping process helps identify which courses cover specific areas of knowledge, and ensures that there is no duplication of efforts. By leveraging the resources and expertise available within the partner offerings, the programme can avoid redundancy and take a synergistic approach to cybersecurity education and training. This approach promotes collaboration and knowledge sharing among the partners, fostering innovation that is in light of the ever-evolving landscape of cybersecurity, where new threats and challenges arise regularly.

In order to maintain focus and coherence within the CyberSecPro education and training programme, any course offerings that could not be mapped to the selected knowledge areas are omitted. This ensures that the programme stays aligned with its objectives and goals. The omission of these courses allows the programme to remain focused on delivering comprehensive and relevant cybersecurity education and training.

The comprehensive table, along with the detailed analysis, is available in Annex A.

## 3.3 Selected Education and Training Modules

This section presents the selected CyberSecPro education and training modules mapped to the selected knowledge areas by partner.

**Penetration Testing (21 offerings)**

| Selected CyberSecPro training modules | CyberSecPro Partner |
|---|---|
| Network and Application Security<br>Cybersecurity Analyst<br>The Landscape of Hybrid Threats<br>Cybersecurity Hackathon Project<br>Cybersecurity Project | LAU |
| Penetration Testing/Malware Analysis<br>Software Security<br>Cyber Security Exercises | URPC |
| Security scenarios: Red and Blue Teaming<br>NMAP - Reconnaissance and Vulnerability Assessment | PDMFC |
| Penetration Testing/Malware Analysis<br>Red Teaming Course/CTF | FP |
| Penetration Testing/Malware Analysis<br>Software Security | Trustilio |
| Security of Systems and Services | TUC |
| Introduction to Cyber Security (Maritime) | TalTech |
| System Security | UCY |
| Thinking like an attacker | SINTEF |

**Cybersecurity Tools and Technologies (40 offerings)**

| Selected CyberSecPro training modules | CyberSecPro Partner |
|---|---|
| Enterprise Security and Practitioners<br>Cybersecurity Working Life Practices<br>Cybersecurity Hackathon Project<br>Cybersecurity Project<br>Network and Application Security<br>Cybersecurity Analyst<br>Internet Infrastructure and Security<br>Network Applications<br>Introduction to Information Security | LAU |
| Information & Communication Security | GUF |
| Information Systems Security<br>Cybersecurity (Hellenic Air Force) | URPC |

| | |
|---|---|
| Network and Communications Security<br>Network Security (Hellenic Air Force) | |
| Security Scenarios: Red and Blue Teaming<br>Privacy and Security Logging, Network Traffic Analysis<br>Log Parsing<br>YARA and SIGMA: Advanced Malware Analysis and Incident Detection<br>Applied Cryptography with GPG and OpenSSL<br>Network Traffic Analysis and Monitoring with Tshark and NFStream<br>Privacy Threat Modelling, Incident Handling - Security Information and Event Management<br>Intrusion Detection and Prevention Systems (IDPS)<br>Identity Access Management | PDMFC |
| Security of Systems and Services | TUC |
| Introduction to Cyber Security (Maritime)<br>Strategic Communications and Cybersecurity<br>Cyber Incident Handling<br>Cyber Defense Monitoring Solutions | TalTech |
| Software Analysis | UCY |
| Secure Coding<br>Digital Identity and Privacy<br>Security in Services and Applications<br>Information Security<br>Security in Services and Applications<br>Security and Privacy in Application Environments<br>Security in Industrial and Cyber – Physical systems<br>Malware Analysis<br>Design and Configuration of Secure Network Systems | UMA |
| Network and Computer Systems Security<br>Cybersecurity and Governance<br>Regional Dynamics of Security and Defense<br>Economic and Competitive Intelligence<br>Methodology and Techniques for Analysis and Prospection | FCT |

**Cybersecurity Management (23 offerings)**

| **Selected CyberSecPro training modules** | **CyberSecPro Partner** |
|---|---|
| Information Security Management<br>Cybersecurity Management<br>Information and Cyber Security Management<br>Information and Cyber Security<br>Introduction of Information Security | LAU |
| Information & Communication Security | GUF |

| | |
|---|---|
| Cybersecurity (Hellenic Air Force) | URPC |
| Risk Assessment and Management<br>Security Scenarios: Red and Blue Teaming<br>Privacy and Security Logging<br>Network Traffic Analysis<br>Log Parsing<br>Identity Access Management | PDMFC |
| Security of Systems and Services | TUC |
| Introduction to Cyber Security (Maritime)<br>Strategic Communications and Cybersecurity<br>Cyber Incident Handling | TalTech |
| Advanced Risk Assessment | AIT |
| Globalisation and Security Risks<br>Software Security<br>Cybersecurity and Governance<br>Cybersecurity<br>Cybercrime - Prevention and Forensic Technique | FCT |

**Cybersecurity Threat Management (31 offerings)**

| **Selected CyberSecPro training modules** | **CyberSecPro Partner** |
|---|---|
| Cybersecurity Working Life Practices<br>Cybersecurity Hackathon Project<br>Cybersecurity Project<br>Systems Security<br>Cybersecurity Analyst | LAU |
| Security Governance<br>Information Security Governance<br>Human-centric risk management<br>Maritime Cyber Security | URPC |
| Risk Assessment and Management<br>Security scenarios: Red and Blue Teaming<br>Privacy and Security Logging<br>Network Traffic Analysis<br>YARA and SIGMA: Advanced Malware Analysis and Incident Detection<br>Lynis<br>OpenSCAP - Security Auditing and Hardening Tools<br>Android Security and Log Parsing | PDMFC |
| Maritime Cyber Security | FP |
| Human-centric risk management | Trustilio |

| | |
|---|---|
| Security of Systems and Services | TUC |
| Introduction to Cyber Security (Maritime)<br>Strategic Communications and Cybersecurity<br>Cyber Incident Handling<br>Cyber Defense Monitoring Solutions | TalTech |
| Information Security and Computer Forensics<br>Computer Forensics<br>Security in Technological Environments<br>Security in Industrial and Cyber - Physical Systems | UMA |
| Software Security<br>Cybersecurity<br>Globalisation and Security Risks | FCT |

**Cybersecurity Risk Management (31 offerings)**

| **Selected CyberSecPro training modules** | **CyberSecPro Partner** |
|---|---|
| Information Security Management<br>Risk Manager<br>Risk, Safety and Security Management<br>Cybersecurity Working Life Practices<br>Cybersecurity Project<br>Systems Security | LAU |
| Security Governance<br>Information Security Governance<br>Human-centric risk management<br>Maritime Cyber Security<br>Software Security | URPC |
| Risk Assessment and Management<br>Privacy Threat Modelling<br>Lynis<br>OpenSCAP - Security Auditing and Hardening Tools<br>NMAP - Reconnaissance and Vulnerability Assessment | PDMFC |
| Maritime Cyber Security | FP |
| Human-centric risk management<br>Software Security | Trustilio |
| Security of Systems and Services | TUC |
| Introduction to Cyber Security (Maritime)<br>Strategic Communications and Cybersecurity<br>Cyber Incident Handling | TalTech |

| | |
|---|---|
| Governance Risk Compliance<br>Advanced Risk Assessment | AIT |
| Cybersecurity<br>Globalisation and Security Risks<br>Digital Transformation in a Cybersecurity context<br>Cybersecurity, IT Asset Management, and Governance<br>How to implement an Information Security Management System with ISO/IEC 27001 | FCT |
| Introduction to Cyber Security: Risk Management | SINTEF |

**Cybersecurity Policy, Process, and Compliance (26 offerings)**

| **Selected CyberSecPro training modules** | **CyberSecPro Partner** |
|---|---|
| Information Security Management<br>Risk Manager<br>Systems Security | LAU |
| Mobile Business II–Technology, Markets, Platforms, and Business Models | GUF |
| Security Governance<br>Information Security Governance<br>Human-centric risk management<br>Maritime Cyber Security<br>Software Security | URPC |
| Risk Assessment and Management<br>Log Parsing<br>Privacy Threat Modelling<br>Lynis<br>OpenSCAP - Security Auditing and Hardening Tools<br>Identity Access Management | PDMFC |
| Maritime Cyber Security | FP |
| Security of Systems and Services | TUC |
| Introduction to Cyber Security (Maritime)<br>Strategic Communications and Cybersecurity<br>Cyber Incident Handling | TalTech |
| Governance Risk Compliance<br>Advanced Risk Assessment | AIT |
| Cybersecurity<br>How to implement an Information Security Management System with ISO/IEC 27001 | FCT |

| | |
|---|---|
| Globalisation and Security Risks<br>GDPR: Governance, Implementation, Maintenance and Control | |

**Cyber Incident Response (28 offerings)**

| **Selected CyberSecPro training modules** | **CyberSecPro Partner** |
|---|---|
| Cybersecurity Working Life Practices<br>Cybersecurity Hackathon Project<br>Cybersecurity Project<br>Business Continuity<br>Environmental Risk Management<br>The Landscape of Hybrid Threats<br>Enterprise Security and Practitioners | LAU |
| Maritime Cyber Security<br>Cyber Security Exercises | URPC |
| Security scenarios: Red and Blue Teaming<br>Log Parsing<br>YARA and SIGMA: Advanced Malware Analysis and Incident Detection<br>Network Traffic Analysis and Monitoring with Tshark and NFStream<br>Android Security and Log Parsing<br>Incident Handling - Security Information and Event Management<br>Intrusion Detection and Prevention Systems (IDPS) | PDMFC |
| Maritime Cyber Security<br>Cyber Defense Exercise<br>Cyber Defence eXercise for Navy (CDX-N) | FP |
| Security of Systems and Services | TUC |
| Introduction to Cyber Security (Maritime)<br>Strategic Communications and Cybersecurity<br>Cyber Incident Handling | TalTech |
| Malware Analysis | UMA |
| Cybersecurity Threat Hunting<br>Governance Risk Compliance<br>Security Incident and Event Management | AIT |
| Cybersecurity and Governance<br>GDPR: Governance, Implementation, Maintenance and Control | FCT |

**Network and Communication Security (29 offerings)**

| **Selected CyberSecPro training modules** | **CyberSecPro Partner** |
|---|---|

| | |
|---|---|
| Data Networks and Information Security<br>Network and Application Security<br>Internet Infrastructure and Security<br>Network Applications | LAU |
| Mobile Business I–Technology, Markets, Platforms, and Business Models<br>Mobile Business II–Technology, Markets, Platforms, and Business Models | GUF |
| Information Systems Security<br>Network and Communications Security<br>Network Security (Hellenic Air Force) | URPC |
| Network Traffic Analysis and Monitoring with Tshark and NFStream<br>Privacy Threat Modelling<br>NMAP - Reconnaissance and Vulnerability Assessment | PDMFC |
| Computer Organization<br>Advanced Computer Architecture<br>Security of Systems and Services | TUC |
| Introduction to Cyber Security (Maritime)<br>Strategic Communications and Cybersecurity<br>Cyber Defense Monitoring Solutions | TalTech |
| Data Security | UCY |
| Information Security<br>Design and Configuration of Secure Network Systems<br>Security in Technological Environments<br>Information Security and Computer Forensics<br>Security and Networks in Online Transactions<br>Security and Privacy in Application Environments<br>Security in Industrial and Cyber-Physical Systems | UMA |
| System and Network Security<br>Security Operations Center | AIT |
| Network and Computer Systems Security<br>Social Network Intelligence | FCT |

**Privacy and Data Protection (25 offerings)**

| **Selected CyberSecPro training modules** | **CyberSecPro Partner** |
|---|---|
| Information Management and Databases<br>Systems Security<br>Introduction to Information Security<br>Information Security Management<br>Risk Manager<br>Systems Security | LAU |

| | |
|---|---|
| Mobile Business I−Technology, Markets, Platforms, and Business Models<br>Mobile Business II−Technology, Markets, Platforms, and Business Models<br>Information & Communication Security | GUF |
| Privacy and Security Logging<br>Network Traffic Analysis<br>Applied Cryptography with GPG and OpenSSL<br>Android Security and Log Parsing<br>Identity Access Management | PDMFC |
| Security of Systems and Services | TUC |
| Introduction to Cyber Security (Maritime)<br>Strategic Communications and Cybersecurity | TalTech |
| Digital Identity and Privacy<br>Security and Privacy in Application Environments | UMA |
| Software Security<br>Data Protection and Management Law<br>GDPR: Governance, Implementation, Maintenance and Control<br>Cybersecurity, IT Asset Management, and Governance<br>The Legal Framework of the Digital Ecosystem - Telecommunications, Media and Information Technology (TMT) | FCT |

**Human Aspects of Cybersecurity (25 offerings)**

| **Selected CyberSecPro training modules** | **CyberSecPro Partner** |
|---|---|
| Enterprise Security and Practitioners<br>Information Security Management<br>Cybersecurity Management<br>Information and Cyber Security Management<br>Information and Cyber Security<br>Cybersecurity Working Life Practices<br>Cybersecurity Hackathon Project<br>Cybersecurity Project<br>Introduction to Information Security<br>Crime Prevention<br>The Landscape of Hybrid Threats | LAU |
| Mobile Business II−Technology, Markets, Platforms, and Business Models | GUF |
| Security Governance<br>Information Security Governance<br>Human-centric risk management<br>Maritime Cyber Security | URPC |

| | |
|---|---|
| Applied Cryptography with GPG and OpenSSL<br>Privacy Threat Modelling<br>Identity Access Management | PDMFC |
| Maritime Cyber Security | FP |
| Human-centric risk management | Trustilio |
| Security of Systems and Services | TUC |
| Introduction to Cyber Security (Maritime)<br>Strategic Communications and Cybersecurity | TalTech |
| Secure Coding | UMA |
| Globalisation and Security Risks | FCT |

## 3.4 Pedagogical Aspects

In order to enhance the quality of the selected education and training modules, specific pedagogic approaches have been identified that hold vital significance for the CyberSecPro education and training programme. These approaches can be effectively utilised in WP3 and WP4 to foster the continuous improvement and development of training modules.

Each individual, with a set of abilities, learns in a different way and receives and develops knowledge differently from others. This theory, known as multiple intelligences, was defined by Gardner and his collaborators of the Harvard University in 1983 [17]. They announced that human beings develop several types of intelligences, each of which encompasses a series of skills that go beyond intellectual capacity, even though the learning process partly involves that part of abstract thinking. Specifically, eight types of intelligences were identified: linguistic, logical-mathematical, musical, visual-spatial, kinesthetic-bodily, intrapersonal, interpersonal and naturalistic [18]. As is evident, all these abilities or intelligences are part of each person, but each person develops or enhances one of these abilities more than the others, all having the same value and importance.

These eight intelligences or ways of thinking lead to different ways of achieving learning, and the need to apply different ways of reaching the individual through multiple types of methodologies and pedagogical approaches. By attending to these intelligence factors, it is possible to create dynamic and purposeful teaching methodologies, in which it is possible to achieve: personal motivation, personalized learning and diversity without condition and limits. Training modules could be more personalized according to the characteristics of each person as well the type of subject matter to be learned. If this is considered, it would then be possible to find innovation by adapting suitable materials (e.g. with attractive activities, formats and languages), pedagogical strategies and methodologies.

For that reason, CyberSecPro adopts a technology-driven, agile methodological approach to intensify learning in the best possible way to each person. Classroom activities and online material will be facilitated by experienced academics and industrial entities who will explore the tasks further and provide group and individual support to trainees, always looking at the value of practice and its usefulness. CyberSecPro training modules aims to enhance the technical capabilities of learners but also of other trainees from the industry (and specifically from maritime, energy, health sector). The programmeis being designed to respond to the needs of the society and accommodate greater flexibility and lifelong learning. The curriculum design and delivery will embrace and recognise any prior learning individuals have achieved and will cater for those who wish to take a stepped-up approach to their goals.

The learning process should therefore be dynamic, adjusting to the particular characteristics of each individual and his/her way of learning new concepts and expanding his or her capabilities.

In the following, the methodologies of flipped classroom and inclusive pedagogy will be presented in light of the CybeSecPro scope. Inclusive pedagogy is at the core of the current project. CyberSecPro will go beyond 'additional needs', as this term is used in a negative way on many occasions. The project will aim to develop such inclusive practices that will not only focus on individuals who have already been identified as having additional needs, but will focus on everybody in the community of the training module.

Whilst inclusive pedagogy is often concerned with those individuals who are 'less able', CyberSecPro will be a pioneer in offering alternative pedagogical advancements that will extend the availability of opportunities to learn and will remove marginalization due to characteristics and individual needs by developing an underpinning framework to transform traditional approaches. The aims of this approach can be broken down into the following categories:

*a) Inclusive Participation*: By placing emphasis on participation, and on collaborative and interactive hand son learning, it will remove any existing knowledge or other type of barriers and inclusive practices will be available to all trainees.

*b) Interactive Learning*: The CyberSecPro inclusive pedagogical approach removes the notion that individuals have a fixed 'ability' to learning. Instead, it will endeavor to focus on those pedagogical approaches that can alter an individual's capacity to learn. It will develop such strategies that can support all trainees equally and remove any stigma.

In order to provide a comprehensive understanding, the two aspects of inclusive pedagogy will be examined individually.

### 3.4.1 Flipped Classroom

A flipped classroom is an instructional strategy and a type of blended learning, which aims to increase learner engagement and learning by having learners' complete readings at home and work on live problem-solving during class time [19] In a flipped classroom, learners are first introduced to new content outside of class, typically through pre-recorded videos, online lectures, or readings, which they review at their own pace. Classroom time is then dedicated to interactive, collaborative, and applied learning activities. A teacher's interaction with learners in a flipped classroom can be more personalized and less didactic, and learners are actively involved in knowledge acquisition and construction as they participate in and evaluate their learning [20]. Some of the benefits of a flipped classroom are [21]:

- It is flexible
- Learners can learn at their own pace
- Learners take responsibility for their learning
- Learners learn rather than encounter material in class
- There are more opportunities for higher level learning
- It does not waste time transferring information to learners when that information is available to them in books or online
- Instructors work more closely with learners, getting to know learners better and providing better assistance
- Increased collaboration between learners

Here is how the flipped classroom works:

*Pre-Learning*: Learners engage with the instructional materials before coming to class. They have the opportunity to attend video lectures, go through relevant materials, or access online resources to gain an

initial understanding of the CyberSecPro material. This activity can be performed anywhere with access to internet.

*In-Class Application*: Classroom time is used for active learning experiences that build upon the pre-learning phase. The learners, instead of passively listening to lectures, they participate in discussions, problem-solving activities, group projects, experiments, or hands-on tasks. The teacher facilitates these activities, providing guidance, clarification, and individualized support as needed.

*Collaboration and Interaction*: In-class activities often involve group work, discussions, and cooperative learning tasks. Learners have the opportunity to share ideas, ask questions, and learn from their classmates.

*Individualized Support*: With the flipped classroom model, teachers can provide more individualized support to learners during in-class activities. They can address learners' questions, provide feedback, and offer one-on-one assistance. This personalized attention helps learners deepen their understanding of the cybersecurity material and overcome potential challenges.

*Application and Higher-Order Thinking*: The flipped classroom approach emphasizes the application of knowledge and the development of higher-order thinking skills. In-class activities focus on problem-solving, critical thinking, and the practical application of concepts. Learners have the opportunity to analyze, evaluate, and synthesize information in a collaborative learning environment.

*Flexibility and Differentiation*: The flipped classroom offers flexibility in the learning process. Learners can review the pre-learning materials on cybersecurity at their own pace multiple times if that is needed. In this way different learning styles or preferences can be served. Moreover, the teachers can apply differentiated instructions based on learners' readiness levels and provide additional support or challenges as required.

The flipped classroom approach can enhance learner engagement, foster deeper understanding, promote critical thinking skills, and facilitate a learner-centered learning environment. By utilizing technology to deliver the cybersecurity content outside of class and using valuable class time for active learning and interaction, the flipped classroom model aims to optimize the learning experience for learners.

### 3.4.2 Inclusive Participation

Inclusive participation learning represents a paradigm shift in education that prioritizes the recognition and accommodation of diverse learning needs and experiences. This approach is grounded in the belief that all learners should have equal opportunities to learn and succeed, regardless of their individual differences, including those related to race, gender, socioeconomic status, cultural background, ability, or learning style [22]. Inclusive education begins with the assumption that all learners have a right to be in the same educational space [23] [24]. It is about creating environments where every learner feels valued and has their learning needs met [25]. This approach requires educators to consider a broad range of strategies and interventions to support diverse learners, from differentiated instruction and universal design for learning to socio-emotional support and culturally responsive pedagogy. Inclusive learning is a paradigm shift in education that prioritizes the recognition and accommodation of diverse learning needs and experiences. This approach is grounded in the belief that all learners should have equal opportunities to learn and succeed, regardless of their individual differences, including those related to race, gender, socioeconomic status, cultural background, ability, or learning style.

Inclusive teaching is relevant to all disciplines, regardless of subject matter, and describes a foundational intention that can take the form of many different techniques and pedagogical approaches. When designing a course, each move matters. From the selection of course materials to teaching methods, to the ways learners are asked to demonstrate their learning, courses may privilege some learners while disadvantaging others. There are moves instructors can make during the course design phase, such as using a diversity statement, creating a syllabus that is accessible and inclusive, and using inclusive language. Several studies [26] converge to the conclusion that it is not enough to guarantee diverse learners access to education, it is also necessary to provide appropriate support to ensure their inclusion.

Effective strategies include applying:

***Universal design principles (UDL)*** to make course materials and learning experiences accessible and welcoming to all learners [27]. Curriculum, as defined in the UDL literature, consists of four parts: instructional goals, methods, materials, and assessments. Deployment of UDL strategies aim to to meet diverse learning needs and perspectives, allowing learners various ways to demonstrate their learning, providing information by default, rather than by request, to make supports accessible to all learners, and modeling inclusive language by asking learners about their personal pronouns, using generic language, and acknowledging different lived experiences. All of the above are achieved with the deployment of the three main principles on which the UDL Framework is based on [28]:

Multiple Means of Representation: This principle emphasizes on providing learners with various ways to perceive information. It involves presenting content in a variety formats, such as text, images, audio, and video, to support different learning styles. By offering diverse representations, the learners can access information using in a way that best suits their needs.

- Multiple Means of Action and Expression: This principle emphasizes on providing learners with multiple options for engaging with and expressing their understanding of the content in question. It encourages the use of various tools and media for expression. Learners are also given choices in navigating and interacting with the learning materials, thus enabling them to showcase their knowledge and skills in ways that are most effective for them.
- Multiple Means of Engagement: This principle focuses on reinforcing learner motivation, engagement and interest in learning. It involves offering different options for engaging with the content, such as incorporating interactive activities, real-world examples, simulations, and providing opportunities for collaboration and peer interaction. By tapping into learners' interests, providing relevance, and offering a range of activities, educators can increase learner engagement and promote deeper learning.

By incorporating these principles into instructional design, educators can create more flexible and accessible learning environments that meet the diverse needs of their learners.

*Differentiated Instruction***:** Differentiation is based on the notion of learners' "differences" that exist in all classroom settings, mixed ability or streaming. It is generally accepted that, all classes accommodate learners with great differences in various factors i.e., readiness level, learning style, interests, prior knowledge, experiences, socioeconomic status, personality and social skills. Two main presuppositions must be met in order for teachers to begin differentiating their instruction: (a) adequate knowledge of the subject which is to be taught and (b) a very good knowledge of each learner's characteristics, needs, strengths and so on [29]. Some key elements of the Differentiated Instruction are:

- Flexible Learning: Differentiated instruction offers various pathways for learners to acquire knowledge and skills.
- Individualized Content: The content is adjusted to match learners' readiness levels. Teachers may modify the complexity, depth, or breadth of the curriculum to ensure that it is appropriate and challenging for each learner.
- Varied Assessments: Differentiated instruction recognises that learners may demonstrate their understanding in different ways. Assessments are designed to accommodate diverse learning styles and preferences.
- Ongoing Support: Teachers provide continuous support and feedback to learners. They monitor learner progress closely and make adjustments to instruction as needed.
- Collaborative Learning: Differentiated instruction encourages collaboration and cooperative learning among learners. Group work, peer tutoring, and cooperative projects allow learners to learn from each other, share ideas, and support one another's learning.

Differentiated instruction recognies the individuality of each learner and seeks to address their specific needs in the learning process. By tailoring instruction to meet learners where they are, it promotes greater engagement, motivation, and academic growth.

*Collaborative Learning:* Collaborative learning is defined as when learners achieve a common learning goal, they complete it in a group and are responsible for each other's learning [30]. It involves structured group activities and projects where peers work together to solve problems, share knowledge, and co-construct new knowledge [31]. Collaborative learning encourages active participation, communication, and teamwork, which can benefit all learners, including those with diverse abilities. Teachers can create inclusive collaborative learning experiences by carefully forming heterogeneous groups, providing clear guidelines and expectations, and facilitating discussions and reflections.

Lin [32] outlines some principles of the Collaborative Learning. These are:

- Provide more language practice opportunities
- Improve the Quality of Learner Talk
- Create a Positive Learning Climate [33]
- Promote Social Interaction
- Allow for Critical Thinking

Gamification is another pedagogical methodology that addresses some of these collaborative learning principles [34], as well as professional training [35]. Gamified and competitive events (e.g. hackathons, cyber games, or cyber exercises) and game-based challenges can create collaborative learning atmospheres, where the learning process is mainly based on fun, cooperation, and social interaction. However, their success depends on the nature and design of the game, the type of tools/platforms to lead the serious games, the type of audience and the application scenario [36] [33] [37], and the use combined of methodologies, such as "flipped classroom games" [33] or simulation-based games for experimental learning [38]. If applied accordingly, it is possible to create highly competitive and profitable learning environments in terms of motivation and interaction.

Indeed, collaborative learning can offer numerous benefits. However, it also comes with its own set of challenges.

*Assistive Technology:* Incorporating assistive technology tools and resources can assist learners with disabilities in accessing the curriculum and participating fully in the learning process. This can include text-to-speech software, screen readers, speech recognition software, alternative keyboards, and other assistive devices. Cybersecurity tools will also be used in the teaching of the offered CyberSecPro courses.

*Culturally Responsive Teaching:* Recogniing and valuing the cultural backgrounds and experiences of learners is essential for inclusive learning. Culturally responsive teaching involves incorporating diverse perspectives, examples, and materials that reflect learners' cultural identities in the curriculum. It also includes creating a classroom environment that respects and appreciates different cultures and encourages dialogue and understanding [39]. Cybersecurity is a subject that attracts a great number of learners or trainees, either from the academic world or from the industry, from different origin and background, who CyberSecPro intents to respond in various ways to enhance their technical capabilities.

*Active Learning:* Engaging learners actively in the learning process promotes inclusivity by allowing them to participate actively and contribute their ideas and experiences. Active learning requires that learners engage in meaningful learning activities [40] and that they be accountable for their own learning [41]. To this effect cybersecurity exercises will be provided to the learners or trainees in the delivery of the modules. Benefits of active learning include increased learner engagement, deeper understanding of concepts, improved problem-solving skills, enhanced critical thinking abilities, and better retention of knowledge. Active learning promotes a learner-centered environment that fosters active engagement, collaboration, and the development of higher-order thinking skills. Deployment of active learning targets in the creation of an inclusive classroom where learners feel valued and involved.

*Peer Tutoring:* This involves pairing learners with different abilities to work together on academic tasks. It can help learners develop social skills, build confidence, and improve academic performance [42]. Indeed, Peer review has demonstrated its efficacy as an evaluative strategy, offering numerous

advantages over traditional methodologies. These include enhancing learners' skill acquisition and development, while fostering their ability for self-directed learning [43]. Peer Tutoring is recommended as a means for educational institutions to develop and foster their inclusive ethos because learners with diverse needs receive individualized and timely feedback [44].

*Ongoing Assessment and Feedback:* Implementing continuous assessment and providing timely feedback is crucial for inclusive learning. Formative assessments allow teachers to gauge individual learner progress and adjust instruction accordingly. Providing constructive feedback helps learners understand their strengths and areas for improvement, promoting a growth mindset and supporting their learning journey.

*Building Positive Relationships:* Establishing positive teacher-learner relationships and fostering a sense of belonging is essential for inclusive learning. Teachers can create a supportive and inclusive classroom culture by showing respect, empathy, and understanding to each learner. Individual conferences, regular check-ins, and creating opportunities for peer interaction can help build relationships and foster a positive learning environment.

*Professional Development and Collaboration:* CyberSecPro aim to enhance the technical capabilities of learners but also of other trainees from the industry. Therefore, continuous professional development for teachers and collaboration among educators are key to implementing effective inclusive learning strategies. Teachers can benefit from training, workshops, and resources that enhance their knowledge and skills in creating inclusive classrooms. Collaborating with colleagues and sharing best practices can further support inclusive education [45].

### 3.4.3 Interactive Learning

Interactive learning can be defined as a process incorporating some type of digitally enabled reciprocal action between a teacher or designer and a learner is defined as interactive learning. Access to content, tasks, and issues by at least one human being (a learner) using digital technology (e.g. a computer with Internet access) [46]. is required for interactive learning. It is a method of teaching that actively engages learners in the learning process through active involvement, collaboration, and hands-on experiences. It stresses learner participation in knowledge construction, idea exchange, and interaction with the learning environment. Learners are encouraged to take an active role in obtaining knowledge, problem-solving, critical thinking, and applying concepts in practical scenarios through interactive learning. Within the scope of the CyberSecPro this will be done with the provision suitable exercises within the deployment of the offered cybersecurity modules.

Here are some key principles and characteristics of interactive learning:

*Active Participation*: Interactive learning promotes active participation and engagement from learners. Instead of passively receiving information, learners are actively involved in activities such as discussions, debates, questioning, problem-solving, and hands-on experiments. They contribute, interact, and share their ideas, experiences, and perspectives.

*Collaboration and Peer Interaction*: Interactive learning fosters collaboration and peer interaction. It encourages learners to work together in pairs or groups, engage in collaborative projects, and learn from each other. Collaboration enhances communication skills, teamwork, and social interaction among learners.

*Constructivist Approach*: Interactive learning aligns with the constructivist approach to education, which emphasizes learners' active construction of knowledge. It acknowledges that learners build their understanding through interactions with the environment, peers, and teachers. Interactive learning environments facilitate this construction of knowledge by providing opportunities for exploration, discovery, and sense-making.

*Application and Practicality*: Interactive learning emphasizes the practical application of knowledge and skills. It provides opportunities for learners to apply concepts, theories, and problem-solving strategies in real-life contexts. This helps learners see the relevance and value of what they are learning and enhances their ability to transfer knowledge to new situations.

*Technology Integration*: Interactive learning often incorporates technology as a tool to facilitate engagement and interaction. Digital platforms, multimedia resources, simulations, virtual environments, and online discussions can be used to enhance interactive learning experiences, promote collaboration, and provide access to a wider range of learning opportunities.

*Individualized Support and Differentiation*: Interactive learning recognies the diverse needs and abilities of learners. It provides opportunities for individualized support, differentiation, and scaffolding to ensure that all learners can actively engage and succeed. Teachers can provide tailored guidance, feedback, and assistance based on each learner's unique needs.

*Reflection and Metacognition*: Interactive learning encourages reflection and metacognition, which involves thinking about one's own thinking and learning processes. Learners are prompted to reflect on their understanding, monitor their progress, and make connections between new and prior knowledge. Reflection supports deeper understanding and helps learners become more self-regulated and independent in their learning.

There are two main techniques to deploy interactive learning in educational and training settings. People can learn "*from*" interactive learning programmes and "*with*" interactive learning technologies, respectively. Learning "*from*" interactive learning programmes is sometimes known as computer-based instruction (CBI) or integrated learning systems (ILS). Cognitive tools and constructivist learning environments are concepts used to describe learning "*with*" interactive software programmes. Databases, spreadsheets, semantic networks, expert systems, communications software such as teleconferencing programmes, online collaborative knowledge construction environments, multimedia/hypermedia construction software, Web 2.0 social media, and computer programming languages are examples of cognitive tools. The cognitive tools approach provides learners with interactive tools to utilize for representing and expressing themselves. Cybersecurity tools will be used for this reason. In any case every interactive learning technique must have three crucial components: engagement, interaction, and feedback. First, the learner must be *motivated* to participate with the knowledge to digest, activities to complete, and/or problems to solve that are at the heart of every interactive learning environment, either intrinsically or extrinsically. Second, the learner must be able to interact with the appropriate knowledge, tasks, and challenges in ways that both the learner and the digital system can understand. Third, the digital system must identify the learner's decisions and activities within an interactive learning environment and acknowledge them through meaningful feedback and assessment [47]

Interactive learning, especially as it is integrated with technology, is not without its challenges. One of the main issues is the digital divide – the disparity in access to technology and the internet among learners, often along socio-economic lines. This divide can hinder the effective implementation of technology-mediated interactive learning, particularly in low-income and rural areas. [48] Moreover, the effective integration of technology into interactive learning requires substantial investment in resources, including hardware, software, and training for educators. There can be resistance to such changes, whether due to a lack of familiarity with technology, concerns about increased workload, or skepticism about the efficacy of technology in improving learning outcomes. Nevertheless, the future of interactive learning looks promising. The continued advancements in technology, including artificial intelligence (AI), AR and VR, and machine learning, present exciting new opportunities for enhancing interactive learning, especially in the field of the cybersecurity the expectations of which are very high. AI, for example, can facilitate personalized learning by adapting instructional content to individual learners' needs, while AR and VR can provide immersive, interactive learning experiences that significantly enhance engagement and understanding.

## 3.5 Summary and Discussion

This chapter primarily analysed and mapped CyberSecPro knowledge areas with education and training modules offered by CyberSecPro partners. This mapping was accomplished by analysing CyberSecPro partners' overall module offerings provided (supply side) earlier in the project and prioritised knowledge areas (demand side) reported in this report. The essence of this mapping was to ensure that only partners'

offerings aligning with the target knowledge areas are considered for further analysis and potential inclusion in the CyberSecPro professional training programme. It is worth noting that the mapping is only for CyberSecPro programme specification guidelines and may need further consolidation in the CyberSecPro programme design phase (D3.1) and development phase (D4.1).

CyberSecPro aims to address the cybersecurity workforce skills gap across the EU and operationalise the ECSF, starting with cybersecurity programmes run by consortium members. The idea is to enable HEIs across the EU, especially CyberSecPro partners, to evaluate their cybersecurity programmes to enhance and reposition them to achieve market-oriented capabilities and ECSF's overall goals. This expectation also applies to the CyberSecPro professional training programme. In this regard, it was necessary to re-examine partners' cybersecurity programmes to ensure their education and training modules fulfil the targeted cybersecurity market-oriented capabilities and align with ECSF. Establishing an education and training module selection method that ensures only relevant partners' education and training modules that address CyberSecPro goals is also essential in the CyberSecPro professional training programme.

This chapter implemented a module selection method, resulting in a comprehensive list of cybersecurity education and training modules to be offered by CyberSecPro partners within CyberSecPro. The chapter also provided a rationale for including these CyberSecPro modules in the CyberSecPro professional training curriculum. Implementing the module selection method has led to several education and training modules fulfilling one or more of the prioritised knowledge areas. Consortium members are encouraged to follow a similar approach to enhance their cybersecurity programmes and introduce new modules that operationalise the ECSF while fulfilling market-oriented capabilities and workforce skills demand.

# 4 Constraints and Requirements for Adoption of the CyberSecPro Programme

CyberSecPro aims to increase the quality of the cybersecurity courses and degrees offered by Higher Education Institutes (HEIs) by integrating a more practical, harmonised approach to teaching and learning, aligned with real working-life needs. In order to achieve this challenging objective, it will be necessary to first identify potential barriers that may arise during the adoption of the CyberSecPro programme, enabling us later to come up with possible requirements or countermeasures that address those barriers.

Thus, in the following sections, we will analyse different types of barriers that may affect the adoption of the CyberSecPro programme, which are related to business, technical, legal, social and financial issues:

- **Business barriers** are associated with any limiting factors coming from industrial agents, belonging to Small and Medium-sized Enterprises (SMEs) or large companies. Within these factors, we highlight those that affect the core business activities (e.g. its particular needs/demands), as well as their areas of application, processes, the personnel available to them, etc. Indeed, the representation of SMEs in training processes may, for example, imply the full dedication of personnel to teaching other cybersecurity professionals or interested entities. This dedication may in turn imply a deviation in the business model and serious disruptions in its normal activity.
- **Technical barriers** include constraints associated with the lack of the necessary hardware or software resources for the proper implementation of CyberSecPro training modules, as well as limitations on the technical knowledge and skills of both trainers and learners. For example, educators in HEIs may have limited technical knowledge of new cybersecurity tools, and HEIs often do not provide for continuous education and training of trainers on these tools.
- **Legal barriers** refer to problems or limitations arising from regulatory agencies or academic departments or centres, such as impediments to modifying course syllabus, ethical and privacy issues, or compliance with extremely rigid bureaucratic procedures. For example, the implementation of Public Private Partnerships (PPPs) or agreements between (private-public) sectors may entail a set of legal procedures that may entail certain restrictions for HEIs.
- **Social barriers** are constraints that may arise from the circumstances surrounding a given society or the individuals participating in the CyberSecPro programme. They can range from the particular limitations of each individual (e.g. communication, understanding, socialisation, etc.) to issues of inclusion, gender and acceptance. For example, people usually enter HEI cybersecurity programmes to get an official and recognised degree (MSc. or BSc.), while flexible programme certificates may require altering the mandate of HEIs, changing their legal conditions (also being a legal barrier) and promoting a different mindset of people to gain acceptance.
- **Financial barriers** are associated with purely economic factors. Within this category, the lack of budget that some entities may have or the limitations in finding extra funding may make it more difficult to participate in certain activities. In addition, European HEIs are often public organisations funded by the respective national ministries, so funding for improving or upgrading cybersecurity labs and tools is often very limited.

It is worth pointing out that sometimes it is not trivial to discern the boundaries between barriers. Some barriers may belong to various of the groups simultaneously, as they may share characteristics of several of them. For example, the use of licensed software can be considered as a technical barrier but also as a legal and financial barrier.

To organise the barriers according to stakeholders of the CyberSecPro project, the following approach is proposed in the following sections: (i) the general or common aspects that the HEIs and the industry may have; (ii) the particular problems of the HEIs; and (iii) the problems of the industry in general.

## 4.1 General Constraints and Requirements

From a global perspective, a very important aspect that may significantly affect the development of the CyberSecPro training programme is precisely how to determine **the minimum knowledge or prerequisites** that are necessary to successfully complete certain training modules. Clearly, it is relevant to establish a baseline understanding of ICT and digital frameworks. This ensures that participants have a solid foundation to build upon during the training. Without this basic knowledge, individuals may struggle to comprehend the more complex cybersecurity concepts and techniques taught in the programme. However, more advanced knowledge may be required for other modules. Therefore, it is crucial to assess the participants' prior knowledge and provide any necessary introductory materials or additional resources to fill any gaps.

**Aligning the level of difficulty within the CyberSecPro programme** is also essential to cater to participants with varying levels of expertise. Some individuals may enter the programme with advanced knowledge and skills, while others may be beginners in the field of cybersecurity. It is important to design the programme in a way that challenges and engages advanced learners, while also providing support and resources for those who are new to the contents. This can be achieved by offering different tracks or modules with varying levels of complexity, providing personalised guidance and mentorship, and incorporating self-assessment mechanisms to allow participants to gauge their own progress. In this respect, and related to the previous point, a minimum knowledge base or prerequisites for specific CyberSecPro courses is required for learners to determine the course they need to enrol in.

The difficulty of **aligning the value of different training modules** may also pose a challenge. Each module or activity within the programme offers unique benefits and learning opportunities. For instance, a hackathon provides hands-on experience and encourages problem-solving skills, while a full semester course at a HEI delves deeper into theoretical concepts. Determining the relative worth of these modules and striking a balance in their allocation within the programme can be a complex task. It requires careful consideration of the desired learning outcomes, participants' expectations, and the overall objectives of the CyberSecPro programme.

During the implementation phase of the CyberSecPro programme and beyond, some questions may arise regarding **new technologies or knowledge areas not fully covered** by the training modules. In the future, new professional profiles and competencies not considered so far may appear. Therefore, it is necessary to seek feedback and collaboration between the various stakeholders involved in CyberSecPro, and to review the state of the art and methodologies for their implementation. Also, careful consideration should be given on how to relate the new profiles to an existing Knowledge area or to the creation of a new area, which will be original to CyberSecPro. Similarly, it may be necessary to **dynamically adapt the training modules to the demand**, the constant change of technologies and knowledge areas. This requires to continuously explore the evolution of the market and its new demands, as well as the contents of the training modules and their tools.

The involvement of private and public institutions with **different views and approaches** on what needs to be taught may lead to inconsistent training modules. This lack of consensus may lead to incomplete training programmes that are not in line with real working-life knowledge and skills. It is thus necessary to seek synergies between institutions and the creation of groups of experts for different areas of interest (e.g. external/internal advisory boards) may be extremely helpful in this process, providing recommendations and suggestions. Moreover, the use of official frameworks, such as European Qualifications Framework (EQF), European Cybersecurity Skills Framework (ESCF) and the European e-Competence Framework (e-CF) could also help to converge criteria and ensure that the knowledge,

skills and abilities identified are so far really covered. Indeed, **the use of reference methodologies and frameworks** for the definition of the training modules are essential tools to guide the specification and integration of the training modules. However, it is also required that all the partners of the consortium know in advance of the existence of these methodologies and how to properly implement them in order to define the training modules according to the requirements of the training modules and the prerequisites of the learners to successful complete the CyberSecPro programme.

**The adoption of new tools in the CyberSecPro programme** may introduce additional difficulties. Proprietary tools, while potentially offering advanced functionality, may come with licensing costs or require specialised training. On the other hand, if open-source solutions are chosen, other problems may appear. For example, it may be necessary to use several additional tools to cover all functionalities and required skills. Additionally, it is essential to ensure that any new tools used in the CyberSecPro programme adhere to strict data protection regulations and best practices, especially when dealing with open-source tools. This may involve conducting a thorough assessment of the tools' security features, implementing necessary safeguards, and educating participants to maintain a secure learning environment. Therefore, cybersecurity tools need to be continuously assessed and innovative tools selected to address emerging cybersecurity educational challenges. Procurement practices within the HEIs need to become more dynamic in order to address this challenge.

Another issue, which may be found during the adoption of the CyberSecPro program, is the official issuance and validity of certificates for acknowledging ECTS credits, degree homologation, accreditations to teaching bodies or public administrations, etc. The ideal scenario would be that certificates were issued by external and recognised entities. However, this in turn raises additional difficulties related to how and where to **find, and convince, official bodies in charge of providing specific cybersecurity programme certificates** with a broad coverage and outreach across the whole European territory. To the best of our knowledge, currently, there are no certification authorities at EU level that certify cybersecurity training at any level (e.g. basic, advance, undergraduate, graduate, post graduate) or type (commercial, governmental), which further complicates addressing the problem. For that reason, the most appropriate and feasible solution for now is to explore possible types of certificates that the CyberSecPro consortium itself could issue, assuming the implicit validation limitations that this process could bring in the future.

**The duration and periods in which training courses are offered** is another limiting factor in the sense that courses are not flexible enough to allow learners to take a course when they need it. For example, if someone needs to learn a certain technology or tool, and the related training modules are delivered at a different moment in time, this person may not be able to acquire the necessary competences/skills until the training module is scheduled again. On the other hand, the extension of the training modules may lead to an overload of work for the learners, which may cause them to drop out prematurely. Therefore, it is important to make access to the training modules more flexible over time, and to design time-bound training modules that cover a limited set of competences and skills.

**Language is another general barrier** that must be taken into account. If the languages in which the training modules are offered are limited or not widely spoken, there is a risk that people with training needs will not be able to attend them, even though they are included in the CyberSecPro programme catalogue. To avoid this situation, the possibility of including additional material, subtitles, or any other additional mechanisms (e.g. sign language for hearing-impaired people) that allows learners to acquire these competencies and skills should be considered.

Another problem to be addressed is how to **make the CyberSecPro programme sustainable** beyond the duration of the project. While the project is active, the professionals teaching the training modules are members of the consortium and will therefore have all the support from the project. However, after the project ends, it is likely that the necessary resources will no longer be available to give continuity to the CyberSecPro programme. In this case, it will be necessary to explore funding mechanisms, for

example, through tuition fees or by sponsors interested in this type of continuous training for cybersecurity professionals. Likewise, a change in behaviour and culture will be necessary for cybersecurity trainers in the relevant HEIs to adopt a more entrepreneurial vision in their teaching approach. They must become the enablers of the digital revolution and those who can best prepare students for an innovative digital future.

Last, but not least, the **development of a Dynamic Curriculum Management (DCM) system will entail the additional cost** of deploying an IT infrastructure and an administrator in charge of maintaining the system. One solution to mitigate this technical risk is to allocate a budget to cover resource costs and hire personnel knowledgeable in platform and system deployment for this activity and its maintenance, if possible.

## 4.2 Higher Education Institutes

From an academic perspective, there are other issues that should be considered within the CyberSecPro project, such as the **quality of the contents and the teaching provided**. If the training modules are taught by cybersecurity professionals with the necessary technical skills but limited teaching experience, it could happen that knowledge is not correctly transferred. This, in turn, will prevent practical contents from being incorporated into HEI courses. A countermeasure would be to carefully chose the professionals in charge of training modules. They should not only have the necessary technical skills but also pedagogical competences to effectively transmit the necessary knowledge. In the absence of qualified professionals from the private sector, HEI members may offer some pedagogical training or guidelines. An indispensable tool to detect teaching deficiencies is to carry out questionnaires to evaluate the quality of the training modules and trainers.

Another problem we may find in the development of the project is the **lack of professors in HEIs** with the willingness **to learn new technologies or incorporate practical contents** to existing courses due to multiple reasons (time, schedule, etc.). Possible countermeasures include hiring staff to take over specialised courses (in case the HEI department can afford it), or assisting trainers in the process of learning new technologies or materials. In the latter case, the solution would be to provide training modules complementary to the contents of existing courses, either through webinars, short workshops, or other means or mechanisms that benefit self-learning.

A major problem for HEIs is related to the **limited flexibility of official degrees**. HEIs depend on the programmes agreed upon by different ministries of education or regulatory bodies that ensure the quality of the degrees offered in the member states. This implies that it may not be possible to include new courses or completely re-design existing syllabuses. In case it was possible to include these contents there would be the added problem that the number of hours available in the course is limited - other content stipulated in the course syllabus would have to still be covered. An alternative solution for some universities would be to offer these contents as expert and specialisation courses in addition to the official Bachelor and Master courses. In addition, it is always advisable to explore the possible learning alternatives that the CyberSecPro consortium could provide, either through (new) materials or (ad hoc) specific training modules.

In order to promote the mobility of students between different HEIs, it may be necessary to address the problem of assessing the competences and skills acquired in the respective cybersecurity courses. Some courses, especially those taught in HEIs involved in the CyberSecPro project will have an eminently practical focus, while courses in external HEIs may not necessarily be oriented to the acquisition of practical competences. This may lead to **difficulties when it comes to validating degrees or courses** between HEIs, or pose problems in international mobility programmes. To alleviate this situation, it is advisable that the syllabuses reflect the percentage of practical contents and/or the tools, type of labs or exercises included. In the future, and only if the consortium allows it, HEIs that are not part of the

CyberSecPro project could also apply to the CyberSecPro programme for the validation of the level of practicality of their courses.

**The budget** also limits the correct development of training modules and the integration of practical activities in existing HEI courses. Each institution has a specific infrastructure, and not all HEIs have the same capacity to acquire new hardware or software licenses to accommodate all the students assigned to a class. In addition, there is the added difficulty that the acquisition of these resources can be delayed due to bureaucratic procedures. As a countermeasure, it will be necessary to question these limitations before determining which tools are appropriate for each training module and to consider the possible economic limitations that HEIs may have. Also, the provision of technologies and online access to infrastructures/tools provided by the private sector need to be considered since these could supplement access to resources and allow for faster management of practical exercises.

## 4.3 Industrial Partners

**Lack of expertise**: A significant constraint is the difficulty in understanding which CyberSecPro training modules may be needed to solve specific business-related cybersecurity problems. It may be the case that industrial partners do not have the necessary background to select a training module in a Knowledge area that can help them in their daily operations.

**Limited resources**: Industry priorities are to deliver products and services and meet clients' requests. Cybersecurity is not the priority unless it becomes an obstacle to business activities or reputation. The resources are limited for cybersecurity training. Therefore, the price of cybersecurity education is an important factor.

**Unfamiliar market target**: Cybersecurity industrial partners always seek in expanding their target market. HEIs can represent new target markets to which they can sell their tools and provide practical trainings. However, HEIs are usually governmental bodies and the procurement process and service agreements are different than to the private sector.

Overcoming these constraints necessitates collaborative efforts between the CyberSecPro training providers and the industrial partners. Conducting a comprehensive needs analysis, developing a flexible curriculum that addresses the latest trends, incorporating relevant compliance requirements, generating a business model with affordable pricing options and considering the scalability and assessment of the CyberSecPro programme are vital steps.

By addressing these challenges, industrial partners can successfully adopt the CyberSecPro programme that meets their specific needs and equips their employees with the necessary skills and knowledge to navigate the dynamic cybersecurity landscape.

## 4.4 Summary and Discussion

This section summarises the analysis made in the previous sections and attempts to provide insights into the general constraints as well as those arising particularly in HEIs and industrial partners. For this purpose, we provide below three tables where each constraint is associated with its corresponding countermeasure(s) and limiting factor(s), such as **B**: Business, **T**: Technical, **L**: Legal, **S**: Social, and **F**: Financial.

In table 12 we summarise the general constraints. From this table we can observe that most of the constraints are due to technical issues. The reasons are very diverse, but this is in line with the overarching objective of the project of strengthening the technical practicality of the HEI degrees according to the working-life demand. The transition towards more practical approaches forces the need

for cooperation between strategic sectors (academia and industry) to find ways that help to align the difficulty levels, value and contents of training modules to new demands, technologies and knowledge areas. In this process, individuals (trainers or learners) may have certain personal or technical limitations that in turn may affect learning and/or the acquisition of skills and competencies, forcing in turn the need to establish mechanisms that facilitate the path towards practical approaches.

Although most of the constraints identified are technical, there are also business, social, legal and financial factors that hinder the process of transition to practical approaches. From table 12, it becomes visible that market fluctuations may affect the sustainability of the CyberSecPro programme, the communication and interaction between entities, and the understanding and follow up of the training modules under specific learning materials and tools.

Table 13: General or common barriers and requirements

| Barriers | B | T | L | S | F | Requirements |
|---|---|---|---|---|---|---|
| Need for a minimum knowledge or prerequisites for CyberSecPro programme | | X | | | | • Assess prior knowledge making use of existing mechanisms such as tests, exams, controls, etc.<br>• Provide any necessary introductory materials or additional resources |
| Difficulty in aligning the level of difficulty | | X | | | | • Offer different training modules with varying levels of complexity<br>• Provide personalized guidance and mentorship<br>• Moderately increase the difficulty of the modules<br>• Incorporate self-assessment mechanisms<br>• Establish a set of minimum knowledge bases or prerequisites to select the courses |
| Difficulty in aligning the value of training modules | | X | | | | • Determine the learning outcomes of each training module<br>• Pay attention to participants' expectations and the overall objectives of the CyberSecPro program |
| Difficulty in managing emerging areas of knowledge and professional profiles - during project integration and operation | | X | | | | • Find the appropriate feedback and collaboration between the various CyberSecPro entities<br>• Review the courses and identify the types of competencies/skills to be developed. This entails reviewing the state of the art and methodologies for their association<br>• Explore how to relate the new profiles to an existing Knowledge area or to the creation of a new and original Knowledge area |
| Difficulty in dynamically adapting the training modules to the demand, the constant technological changes, and knowledge areas | X | X | | | | • Explore the evolution of the market, its new demands, the contents of the training modules and tools |
| Difficulty in reaching consensus on training programmes or modules | | X | | X | | • Seek the appropriate synergy between institutions<br>• Create groups of experts |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | • Use existing and standardised methodologies such as ECSF. Always refer to D2.1 |
| Difficulty in applying the new methodologies/frameworks and aligning them with the real demand | | X | | | | • Know about the existence of these methodologies for defining the training modules. Always refer to D2.1 |
| Difficulty in the adoption of new or existing tools (e.g. information and operational tools) | X | X | X | | X | • Evaluate the cost-benefit ratio of new components<br>• Promote the use of (proprietary or open-source) tools under strict data protection measures and best practices - especially when dealing with open-source tools<br>• Guarantee validation and implement necessary safeguards<br>• Educate and raise awareness of data privacy protocols to maintain a secure learning environment |
| Difficulty in finding official bodies for certification of specific security programmes | | | X | | | • Explore the problem and find possible types of certificates that can be issued by the CyberSecPro consortium |
| Difficulty in finding flexible training modules for the community | X | | | X | | • Design flexible training modules over time, and less extensive modules that cover a determined set of competencies and skills |
| Difficulty in following the training modules due to language (communication) | | X | | X | | • Offer additional (language-related) material, subtitles or any other additional mechanisms<br>• In the worst case, provide additional indications or requirements about the minimum conditions to take the course |
| Difficulty in ensuring the sustainability of the CyberSecPro programme in the future | X | X | X | X | X | • Explore funding mechanisms, implying HEIs and private sector<br>• Adopt a more entrepreneurial vision in future HEI teaching approaches |
| Difficulty in deploying and maintaining the DCM platform | | | | | X | • Reserve budget (if required) for resources and qualified personnel in charge of this activity |

In table 13, we focus on the constraints to the design and deployment of CyberSecPro programmes on the academic sector. We observe that most of the constraints are technical and legal issues. The reason for this is partly due to the difficulties in following practical approaches in institutions with static and rigid theoretical programmes, and to the fact that institutions (together with their training programmes) are often regulated and controlled by government agencies under regulatory frameworks to standardise and regulate education within a country.

Table 14: Academic barriers and requirements

| Barriers | B | T | L | S | F | Requirements |
|---|---|---|---|---|---|---|
| Insufficient quality of the contents and the teaching provided | | X | | X | | • Identify suitable personnel, both at the technical and teaching levels (by experience, evaluation, etc.). |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | • Design satisfaction questionnaires to evaluate the quality of the training modules and their trainers<br>• Foster teaching or pedagogical courses/guidelines (provided by HEIs) and methodologies |
| Lack of interest by HEI professors in learning new technologies or incorporating practical content. | | X | | X | | • Hire new staff (in case the HEI Department allows it) or assist professors in learning new technologies or material<br>• Provide complementary training modules to existing content |
| Limited flexibility of official degrees | | | X | | | • Explore the conditions of each HEI, its needs and regulations<br>• Propose non-official university specialization and expert courses |
| Difficulty in validating degrees or courses between HEIs or mobility issues | | | X | | | • Reflect in the syllabuses the percentage (%) of practical content, and/or to detail with precision the tools, type of practices or exercises included<br>• Encourage the participation of external HEIs in CyberSecPro programmes in the future. |
| Difficulty in acquiring new infrastructures, technologies, and licences – budget / delays | X | X | X | | X | • Analyse any economic constraints before designing training modules, in which the tools/infrastructure must be identified<br>• Foster the use of technologies provided by the private sector and online access to external infrastructures/tools (provided by the same sector) |

Table 14 summarises the industrial constraints and requirements, and shows the influence of the main barriers, which are mainly related to business and technical issues, and in which a joint effort between institutions is still required. It is not only necessary to enhance the capabilities of HEIs to drive teaching to current needs, but also to enhance the scientific capabilities of the private sector itself to analyse and identify potential needs.

Table 15: Industrial constraints and requirements

| Constraints | B | T | L | S | F | Requirements |
|---|---|---|---|---|---|---|
| Lack of expertise | | X | | | | • Targeted awareness and consulting to raise the cybersecurity maturity of the industries |
| Lack of resources | X | X | | | | • CyberSecPro programme and modules need to be affordable<br>• The CyberSecPro business and pricing model need to be aligned with the industrial aims |
| Unfamiliar market target | X | | X | | X | • Clear procurement and purchasing procedures are needed |

Finally, Table 15 highlights which domains of barriers (business, technical, legal, social, or financial) most influence the respective entities, as well as the domains that follow them. This way, it is also

possible to identify which actions should be carried out within the project to prioritise efforts and avoid, as far as possible, their possible negative influences. The table also shows that most of the barriers identified in this section belong to the technical domain. However, this does not necessarily mean that these are the most important obstacles or that they are the ones that should be tackled first. Generally, technical barriers are more easily addressed than other types of barriers. For example, legal and social barriers may be beyond our reach and may be determinant for the correct development of the project.

Table 16: Main barriers affected per entity/entities

| **Entity / entities** | **Main barriers affected** | | | | | **Followed by** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **B** | **T** | **L** | **S** | **F** | **B** | **T** | **L** | **S** | **F** |
| HEIs and industrial partners | | X | | | | X | | X | X | X |
| HEIs | | X | X | | | X | | | X | X |
| Industrial partners | X | X | | | | | | X | | X |

In conclusion, this chapter has explored and analysed various barriers that may hinder the successful adoption of the CyberSecPro education and training programme. It has become evident that these obstacles can stem from a multitude of factors, ranging from technical constraints to financial limitations. This chapter has also explored potential strategies to address the barriers encountered. Ultimately, the successful adoption of the CyberSecPro programme requires a multi-faceted approach, entailing strategic planning, effective communication, and persistent efforts to overcome the barriers identified. We believe that these tables can help guide the design and deployment of training modules in certain application environments (e.g. in HEIs, in private sectors such as energy, maritime or health, public administrations, etc.), and allow the consortium to anticipate situations that may cause a blockage in the implementation, achievement and validation of these modules.

# 5 CyberSecPro Dynamic Curriculum Management System

## 5.1 Introducing DCM systems

A **curriculum management system** (**CMS**) is a software application for the administration, documentation, tracking, reporting, automation, and delivery of educational courses, training programmes, materials or learning and development programmes.

Through the use of data analysis and reports, CMSs are designed to identify gaps in training and learning. They act as platforms for delivering online content, both asynchronous based and synchronous based, and support a range of uses, mostly focused on online training delivery. In the higher education space, a CMS may offer classroom management for instructor-led training or a flipped classroom.

A dynamic curriculum management (DCM) system can help schools and teachers teach new skills through blended learning experiences that integrate new technologies into classroom activities. One of the biggest reasons a dynamic curriculum is so effective is that it allows students to learn at their own pace.

For the CyberSecPro education and training programme to achieve success, it is essential to have a comprehensive understanding of the design and functional requirements of the DCM system. To this end, a comprehensive analysis of requirements will be conducted, serving as the foundation for subsequent stages of development and implementation of the DCM system. The project is adopting an agile approach to accommodate the rapidly evolving cybersecurity landscape and the resulting dynamic requirements, allowing for flexibility in adapting to unforeseen challenges. Consequently, the list of requirements presented in this chapter should be considered preliminary, as it is likely to evolve throughout the project.

Additionally, given that each platform has unique strengths and limitations, it is crucial to select the most appropriate one for the implementation of the CyberSecPro education and training programme. To ensure an efficient selection process for the platform, we will develop a set of high-level criteria. This is crucial because examining all 461 requirements against every DCM system available would be an overwhelming task. By using these high-level criteria, we can conduct a comprehensive assessment of the available CMSs and make an informed decision that aligns with the objectives of the CyberSecPro project. Furthermore, after selecting a CMS, we will compare it with the developed requirements to determine its compatibility. This comparison will help identify areas where the system already fulfils the requirements and areas that require modifications or adaptations. This step ensures that the chosen option meets the necessary criteria and allows us to address any gaps or shortcomings effectively. The process is summarised in Figure 5.

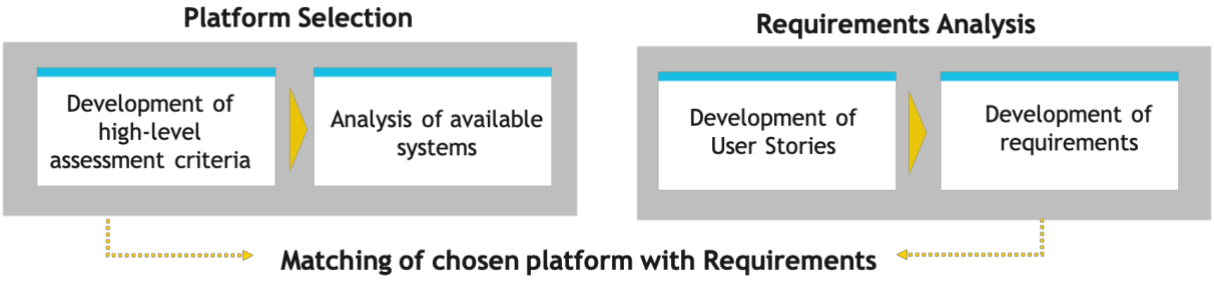



Figure 5: DCM methodology

The remainder of this chapter will be structured as follows: First, the various steps involved in the analysis of the DCM system requirements will be presented. Following, the next section will present assessment criteria that will be used to evaluate and select the most suitable DCM system. These criteria will serve as a framework for assessing the different systems available in the market. This analysis will be presented in the next section and involves a thorough evaluation of various systems, including commercial solutions and open licence solutions. After conducting this analysis, a final system will be

selected based on the developed criteria. Finally, the selected DCM system will be compared against the identified requirements to determine areas where the system already meets the requirements and areas where modifications or adaptations need to be made. This step ensures that the chosen system is able to meet the specific needs of the CyberSecPro education and training programme, while also highlighting any adjustments that may be necessary.

## 5.2 DCM Requirements Analysis

Subsequently, the process followed to derive the requirements for the DCM system is presented. The objective of this process was to identify and analyse the needs and expectations of the different stakeholders involved in the DCM system, namely trainers, trainees, and institutions. By creating and analysing use cases for these user groups, a comprehensive set of requirements for the DCM system was extracted.

The first step in the requirements derivation process involved the creation of user stories by the project partners. User stories are a widely used technique in agile software development to capture user requirements in a concise and understandable manner. The project partners created a significant number of user stories that they found relevant for the DCM system. These user stories were then compared to identify any overlaps or similarities among them. After a thorough comparison and analysis of the generated user stories, a total of 68 user stories were identified for the three different roles in the DCM system: trainers, trainees, and institutions. Additional general user stories that were applicable to all three roles, such as "create account," were also identified.

In the second step, the 68 identified user stories were enhanced and detailed through the use of a standardised use case template, which is available in Annex B. This template provided a structured framework for documenting the use cases associated with each user story. The use case template consisted of the following sections:

1. Brief Description
2. Actors
3. Pre-conditions
4. Basic Flow
5. Alternative/Exception Flows
6. Post Conditions
7. Supplemental Requirements
8. Visual Model

The 68 identified user stories were divided among several partners. The partners filled the use case templates for their assigned user stories, ensuring that all the relevant information was captured. Regular meetings were organised during this process to discuss the progress and address any challenges or issues faced by the partners.

In the last step of the requirements derivation process, the filled use case templates were thoroughly analysed. The objective of this analysis was to extract the requirements for the DCM system based on the information provided in the use cases. During the analysis, the requirements were identified in a systematic and comprehensive manner. The focus was on reducing complexity by consolidating similar requirements into a generic version that could be applied to all application scenarios. This approach aimed to minimise the number of requirements while maintaining their effectiveness and applicability.

As a result, a total of 461 requirements were identified for the DCM system. These requirements were further categorised into four categories:

1. Functional requirements - These are all about what the system should do, like letting people create and manage their accounts. (e.g. “The platform should display a form with editable fields (username, password, email, etc.) for account creation.”)
2. Non-functional requirements - These focus on how the system should work, making sure it's easy to use and runs smoothly. (e.g. “The platform should have an intuitive and clear interface for smooth user navigation.”)

3. Constraint requirements - These lay down the rules, like making sure passwords match. (e.g. “The password entered for confirmation must be correct.”)
4. Supplemental requirements - These are the extras that make the system even better, like user-friendly interfaces for managing reviews. (e.g. “Provide a user-friendly interface for navigating and responding to reviews.”)

In our pursuit of refining system requirements, we strategically employed the MoSCoW Prioritisation technique. MoSCoW categorises requirements into four priority levels:

1. Must-Have (M): These represent requirements that are deemed absolutely essential for the core functionality of the system. They are non-negotiable and form the foundational pillars of the DCM system's operation. Example: "The platform should delete the account after the specified period if not cancelled by the user."
2. Should-Have (S): These requirements enhance the user experience and augment system efficiency, adding significant value to the system. While not indispensable, they are highly desirable. Example: "The platform should be quick and efficient, ensuring instant data retrieval and user responsiveness."
3. Could-Have (C): These requirements encompass valuable features or functionalities, which, while not critical for the initial system deployment, are considered beneficial. Example: "Forums or discussion boards with predefined categories could be created within the DCM."
4. Won't-Have (W): These requirements, while potentially intriguing or appealing, are explicitly deferred or excluded from the current scope of the project.

These meticulously derived and prioritised requirements serve as the cornerstone for the ensuing phases of DCM system development and implementation, ensuring that the system is tailored to meet the specific and exacting needs of the CyberSecPro education and training Program

## 5.3 Assessment Criteria for DCM

When selecting a Learning Management System (LMS) or a Curriculum Management System (CMS), it's crucial to evaluate various criteria to make an informed decision. An overview of the identified criteria is displayed in Figure 6. In the following, a more detailed overview of the important factors to consider is presented [49] [50] [51] [52] [53].

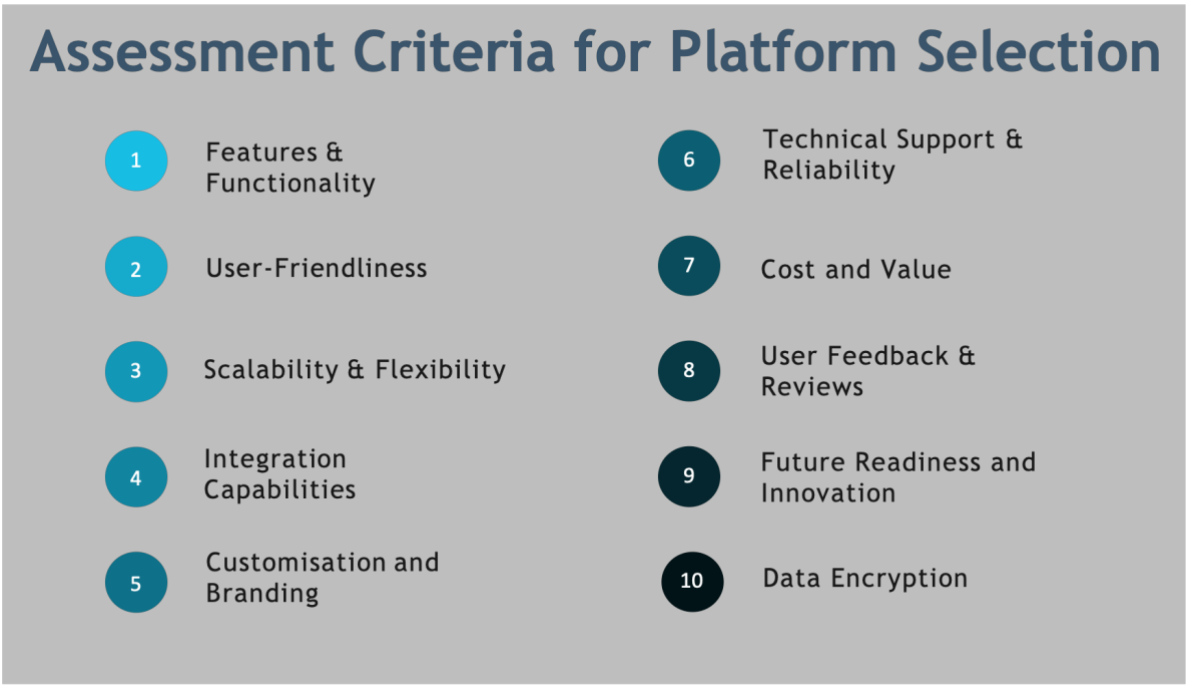



Figure 6: Assessment criteria for platform selection

### 5.3.1 Features and Functionality

Assessing the range of features and functionality offered by a Learning Management System (LMS) or Curriculum Management System (CMS) is crucial to ensure it meets the organisation's requirements. The following aspects need to be considered:

Content Management: A robust LMS or CMS should provide efficient content management capabilities, allowing administrators to organise, upload, and distribute learning materials effectively. Look for features like file management, version control, and content reuse to streamline content creation and management processes.

Course Creation: Evaluate the system's course creation tools. A comprehensive LMS or CMS should support the creation of engaging and interactive courses, offering a variety of multimedia options, such as videos, audio, and images. Look for features like customisable templates, drag-and-drop functionality, and the ability to embed external content.

Assessment Tools: Evaluate the system's assessment capabilities, including support for various question types, automated grading, and advanced assessment options such as rubrics and competency-based assessments. Look for features that facilitate formative and summative assessments, as well as the ability to provide timely feedback to learners.

Communication Tools: Effective communication is vital in an online learning environment. Evaluate the system's communication tools, including discussion forums, messaging systems, and real-time chat functionality. Look for features that promote collaboration and foster active engagement between learners and instructors.

Reporting Capabilities: A robust reporting system enables administrators and instructors to track learner progress, identify areas of improvement, and generate insightful analytics. Look for reporting features such as customisable dashboards, pre-built reports, and the ability to export data for further analysis.

Integration with Other Systems: Consider the system's ability to integrate with other tools and systems used within your organisation. Look for support for interoperability standards like LTI (Learning Tools Interoperability) and APIs (Application Programming Interfaces) to facilitate seamless integration with external systems, such as student information systems, content authoring tools, and learning analytics platforms.

### 5.3.2 User-Friendliness

User-friendliness plays a critical role in ensuring both administrators and learners can navigate and utilize the LMS or CMS efficiently. The following aspects need to be considered:

User Interface: Evaluate the system's user interface for its intuitiveness, clarity, and ease of use. A well-designed interface should provide clear navigation, a logical organisation of features, and an intuitive user experience that minimises the learning curve for new users.

Accessibility: Accessibility is essential to accommodate diverse learners, including those with disabilities. Look for an LMS or CMS that adheres to accessibility standards and offers features such as screen reader compatibility, keyboard navigation support, and adjustable text sizes or colour contrast.

Mobile Responsiveness: With the increasing use of mobile devices, it is important to consider how well the system adapts to different screen sizes and functionalities. Look for a responsive design that ensures optimal user experience across various devices, including smartphones and tablets.

### 5.3.3 Scalability and Flexibility

Scalability and flexibility are crucial factors, especially if your organisation anticipates growth or needs to accommodate varying learning environments. The following aspects need to be considered:

Scalability: Evaluate the system's ability to scale as your organisation grows. Look for features that support a large number of users, courses, and concurrent activities without sacrificing performance. Consider whether the LMS or CMS can handle the anticipated increase in user load and content volume.

Different Learning Environments: Consider the system's flexibility to support various learning environments, such as traditional classrooms, online learning, blended learning, or self-paced learning. Look for features that allow you to create and deliver content for different instructional modes, ensuring a consistent learning experience across different settings.

Course Customisation: Assess the system's flexibility in customising courses to align with your organisation's unique requirements. Look for features that enable instructors to tailor content, assessments, and activities based on learners' needs, as well as the ability to create personalized learning paths.

### 5.3.4 Integration Capabilities

Integration capabilities are essential to streamline workflows and create a cohesive learning ecosystem. The following aspects need to be considered:

Compatibility with Existing Systems: Evaluate the system's compatibility with existing tools and systems used within your organisation, such as student information systems, content authoring tools, video conferencing platforms, or learning analytics tools. Look for out-of-the-box integrations or the availability of APIs to facilitate seamless data exchange and integration.

Single Sign-On: Single Sign-On (SSO) integration allows users to access the LMS or CMS using their existing credentials. This eliminates the need for multiple logins and enhances user experience. Consider whether the system supports popular SSO protocols like SAML (Security Assertion Markup Language) or OAuth.

Data Exchange and Interoperability: Look for systems that adhere to interoperability standards like SCORM (Sharable Content Object Reference Model) or xAPI (Experience API). These standards facilitate the exchange of learning content and data between systems, enabling a seamless flow of information and the ability to track learner progress across different platforms.

### 5.3.5 Customisation and Branding

Customisation and branding options allow you to tailor the LMS or CMS to match your organisation's visual identity and create a cohesive learning experience. The following aspects need to be considered:

User Interface Customisation: Evaluate the system's flexibility in customising the user interface. Look for features that allow you to modify colour schemes, logo placement, and branding elements to create a visually consistent experience for learners.

Course Templates: Assess whether the system allows you to create and customise course templates. This enables instructors to maintain a consistent look and feel across courses, ensuring a cohesive learning experience for learners.

Branding Elements: Look for features that allow you to incorporate your organisation's branding elements throughout the LMS or CMS, such as personalized certificates, customised email templates, and branded course catalogues.

Reporting Formats: Consider whether the system allows customisation of reporting formats. Look for features that enable you to tailor reports to align with your organisation's reporting requirements, including the inclusion of specific data points or visualizations.

### 5.3.6 Technical Support and Reliability

Technical support and reliability are crucial to ensure smooth operation and resolve any issues that may arise. The following aspects need to be considered:

Customer Support: Evaluate the level of technical support provided by the system vendor. Look for options like email support, phone support, or live chat, and assess their responsiveness and availability. Consider whether the vendor offers different support tiers or service level agreements (SLAs) to meet your organisation's needs.

Training Resources and Documentation: Assess the availability of comprehensive training resources, such as user guides, video tutorials, or knowledge bases, to help administrators and instructors learn and navigate the system effectively. Look for well-documented APIs and developer resources if you require custom integrations or extensions.

Software Updates: Consider the vendor's track record of releasing software updates and bug fixes. Regular updates ensure the system remains secure, reliable, and up-to-date with the latest features and industry standards. Look for vendors who actively engage with their user community and incorporate user feedback into their updates.

Uptime and Reliability: System uptime is critical to uninterrupted learning experiences. Evaluate the vendor's track record of system uptime and inquire about their server infrastructure, data backup practices, and disaster recovery measures to ensure the reliability and availability of the LMS or CMS.

Data Security: Assess the system's data security measures, including encryption protocols (such as SSL/TLS) for secure data transmission, user access controls, and compliance with data protection regulations (e.g. GDPR or HIPAA). Consider whether the system undergoes regular security audits or certifications.

### 5.3.7 Cost and Value

Evaluating the cost and value of an LMS or CMS helps ensure that it aligns with your budget and delivers a return on investment. The following aspects need to be considered:

Pricing Model: Assess the system's pricing model, whether it is based on a one-time license fee, subscription, or per-user basis. Consider the total cost of ownership, including any additional costs for support, upgrades, or customisations.

Value Provided: Consider the value provided by the system in terms of its features, scalability, and long-term benefits for your organisation. Look beyond the initial cost and evaluate how the LMS or CMS can support your organisation's goals, improve learning outcomes, and streamline processes.

ROI Analysis: Conduct a cost-benefit analysis or return on investment (ROI) assessment to evaluate the potential financial and non-financial benefits of implementing the LMS or CMS. Consider factors such

as increased learner engagement, reduced administrative overhead, improved training efficiency, and potential cost savings.

### 5.3.8 User Feedback and Reviews

Gathering feedback from current users of the LMS or CMS provides valuable insights into its strengths and weaknesses. The following aspects need to be considered:

User Surveys and Interviews: Conduct user surveys or interviews to gather feedback from administrators, instructors, and learners who have hands-on experience with the system. Ask about their overall satisfaction, ease of use, key strengths, areas for improvement, and any specific challenges they encountered.

Online Reviews and Testimonials: Research online reviews and testimonials from reputable sources or educational communities. These reviews can provide insights into the system's usability, reliability, customer satisfaction, and overall user experience.

Vendor References: Request references from the LMS or CMS vendor to connect with organisations similar to yours that have implemented the system. Speak with their representatives to understand their experiences, challenges, and benefits derived from using the system.

### 5.3.9 Future Readiness and Innovation

Considering the future readiness and innovation of an LMS or CMS ensures that it can adapt to evolving educational needs and incorporate emerging technologies. The following aspects need to be considered:

Vendor Roadmap: Assess the vendor's future development plans and roadmap for the LMS or CMS. Inquire about their commitment to ongoing updates, new feature releases, and support for emerging trends and technologies.

Innovation Track Record: Evaluate the vendor's track record of innovation. Look for evidence of incorporating emerging technologies like mobile learning, gamification, artificial intelligence, adaptive learning, or virtual reality to enhance the learning experience and address future educational needs.

Community and Collaboration: Consider whether the vendor actively engages with the user community through forums, user conferences, or user groups. A strong user community indicates an environment of collaboration, knowledge-sharing, and continuous improvement.

### 5.3.10 Data Encryption

Data encryption is essential to ensure the secure transmission of sensitive information between users and the LMS or CMS. The following aspects need to be considered:

Strong Encryption Methods: Look for systems that employ strong encryption methods, such as SSL/TLS, to encrypt data during transmission. This ensures that user credentials, personal data, and other sensitive information remain protected from unauthorised access or interception.

Data Privacy Compliance: Assess whether the LMS or CMS vendor complies with relevant data privacy regulations, such as GDPR or HIPAA, to safeguard user data. Inquire about their data storage practices, data retention policies, and access controls to ensure data privacy and security.

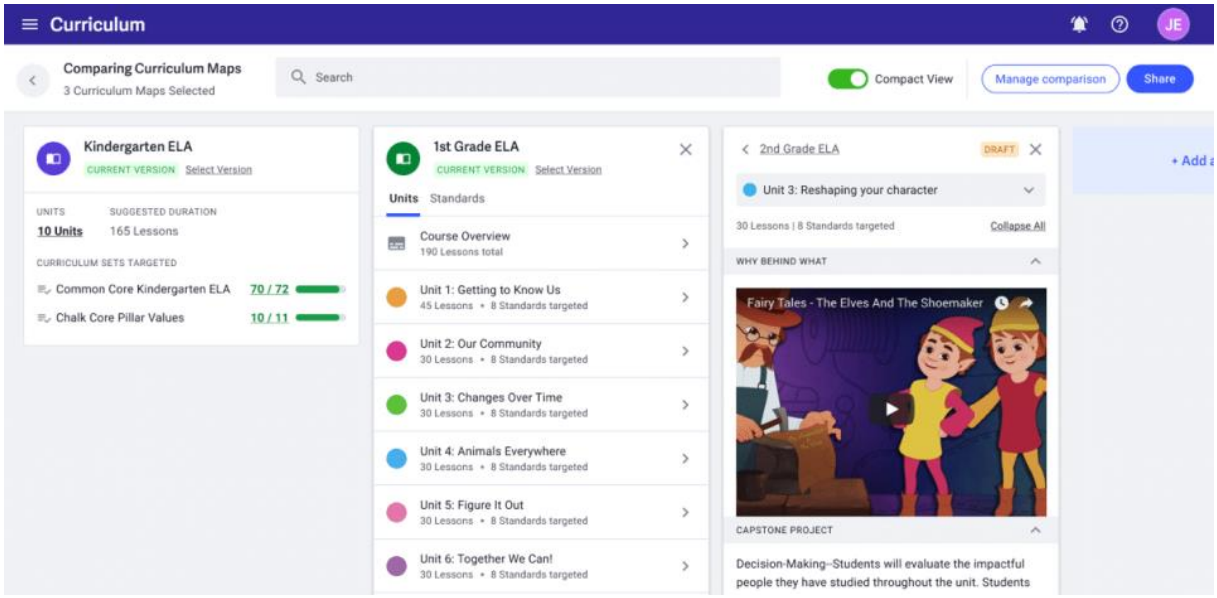
By thoroughly considering these criteria, a well-informed decision can be made concerning the selection of an LMS or CMS that best meets the organisation's unique needs, enhances the learning experience, and supports your long-term goals.

## 5.4 Supply of DCM systems

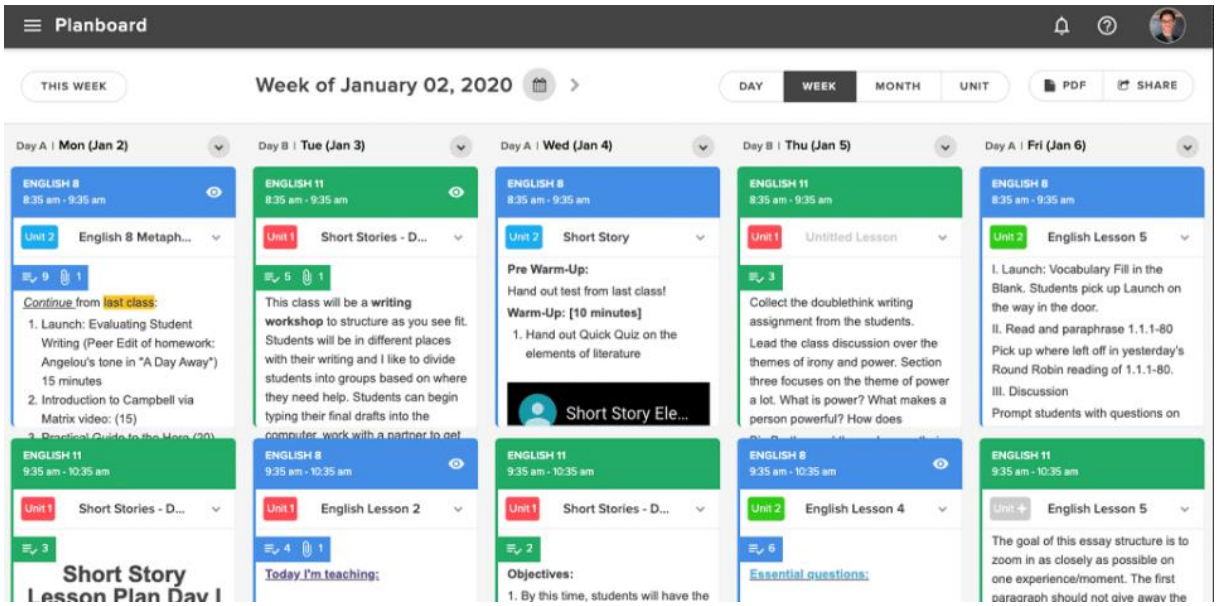
### 5.4.1 Commercial Solutions

PowerSchool Unified Classroom - PowerSchool Unified Classroom® | PowerSchool

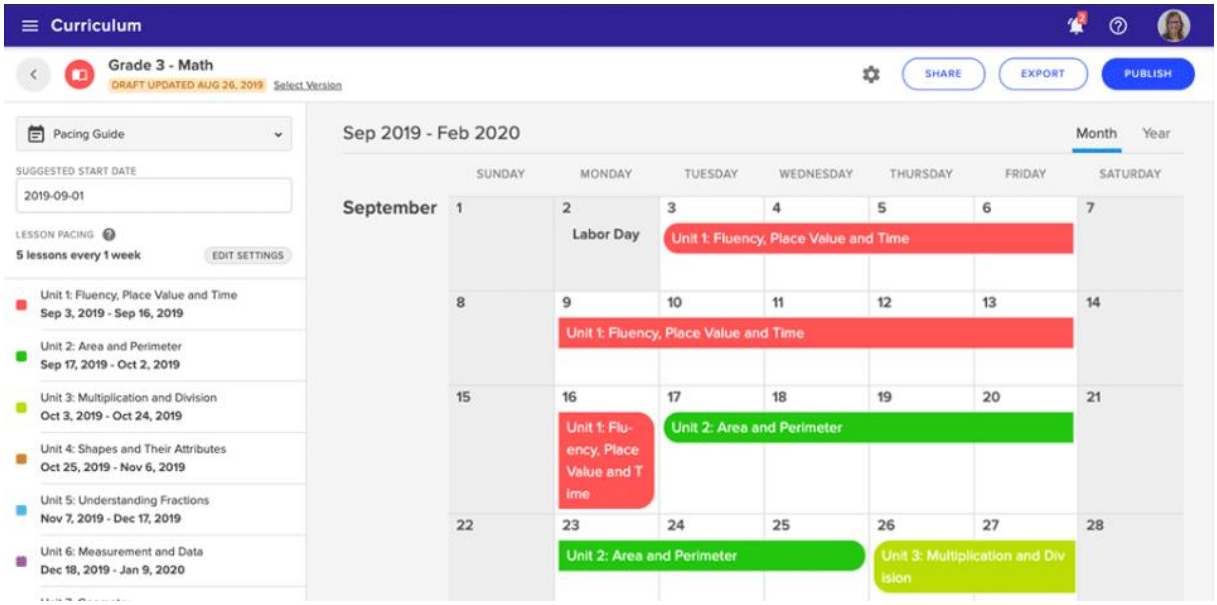
PowerSchool Unified Classroom is a learning management software designed to help K-12 educational institutions manage teaching sessions, assessments, and collaboration. The platform lets administrators create custom assessments to evaluate students via automated scoring of quizzes, unit or district benchmark assessments, and psychometric data.




Screenshot 1: PowerSchool Unified Classroom



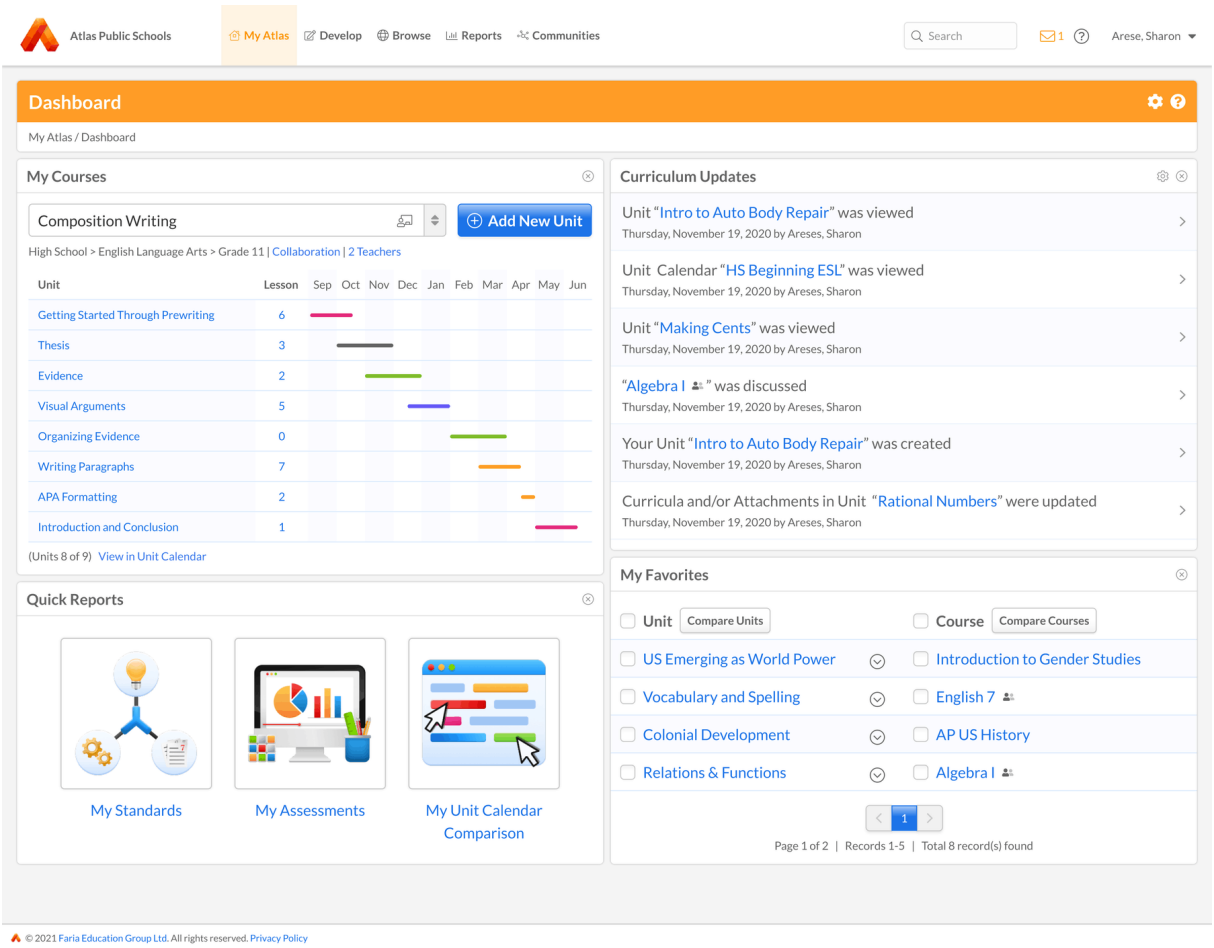

Screenshot 2: PowerSchool Unified Classroom




Screenshot 3: PowerSchool Unified Classroom

Atlas Curriculum Management - Atlas (onatlas.com)

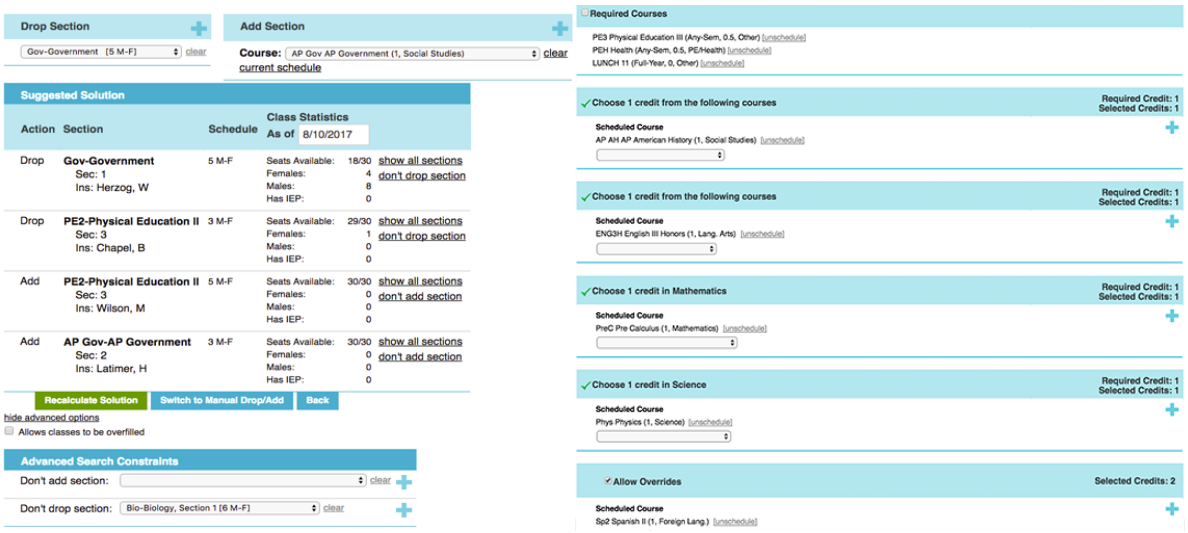
Atlas School Curriculum software helps schools initiate, re-design, and continually refine and improve curriculum development processes in a single unified system. By offering a seamless and integrated experience, the Atlas curriculum planning platform lets schools manage different types of curriculum design for the same course. It also provides unit planner templates that are designed to evolve with your curriculum development.




Screenshot 4: Atlas Curriculum Management

Schoolinsight - Standards-based Learning and Student Information System - Common Goal Systems, Inc (schoolinsight.com)

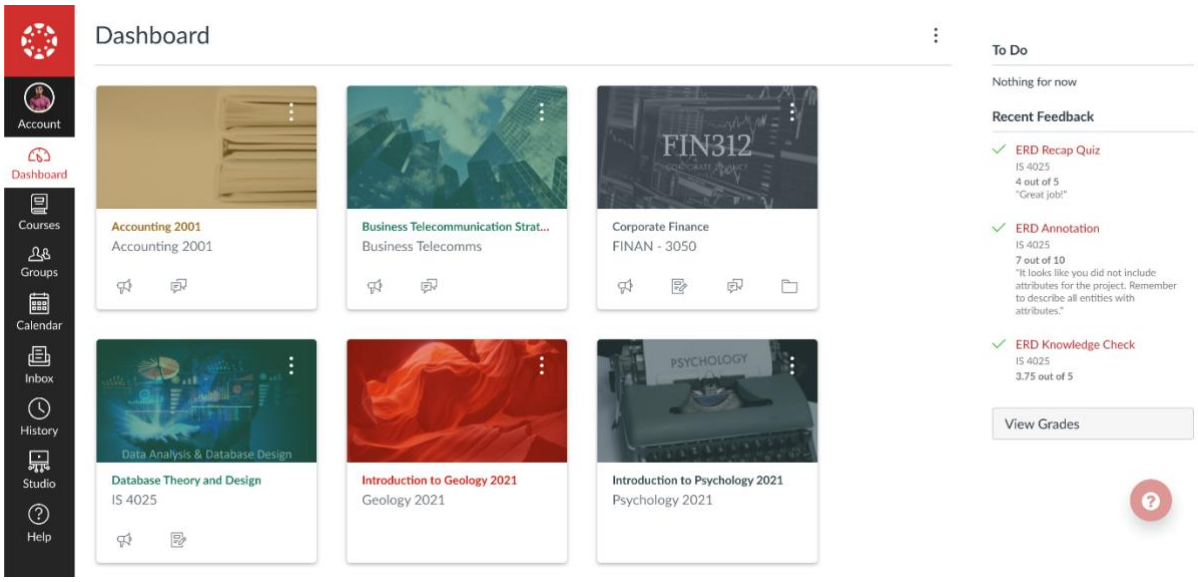
Includes the software tools required to manage most small-to-medium sized districts and non-public schools: student demographics, basic scheduling, attendance, grade reporting (report cards/transcripts), and tuition/fees.



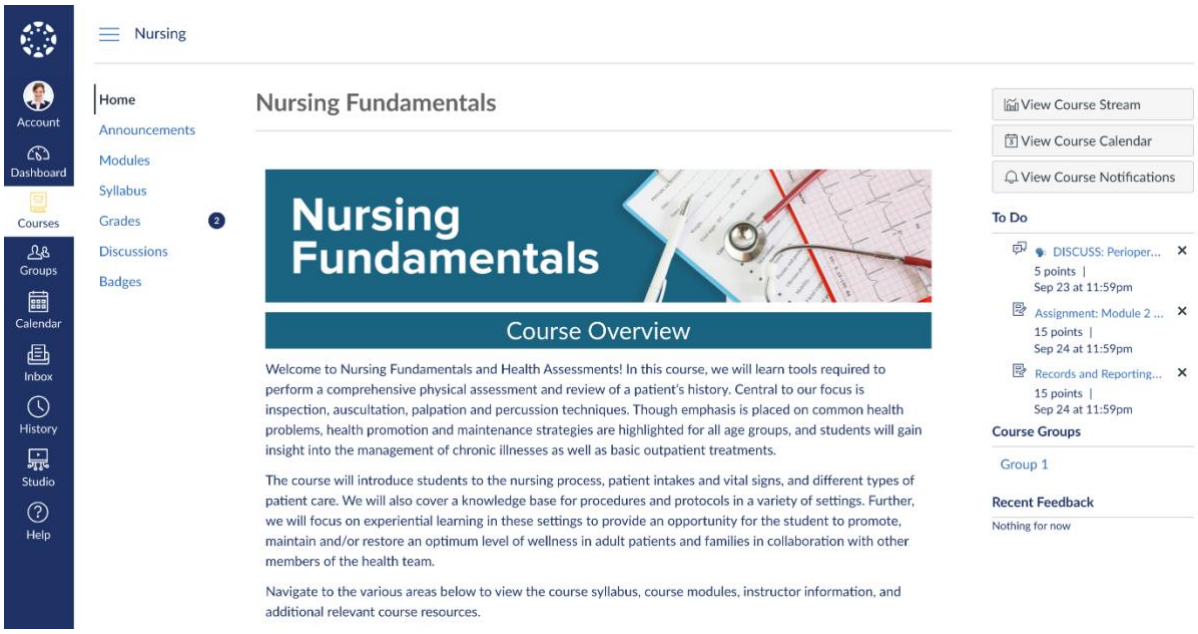

Screenshot 5: Schoollinsight

## Canvas - Canvas by Instructure

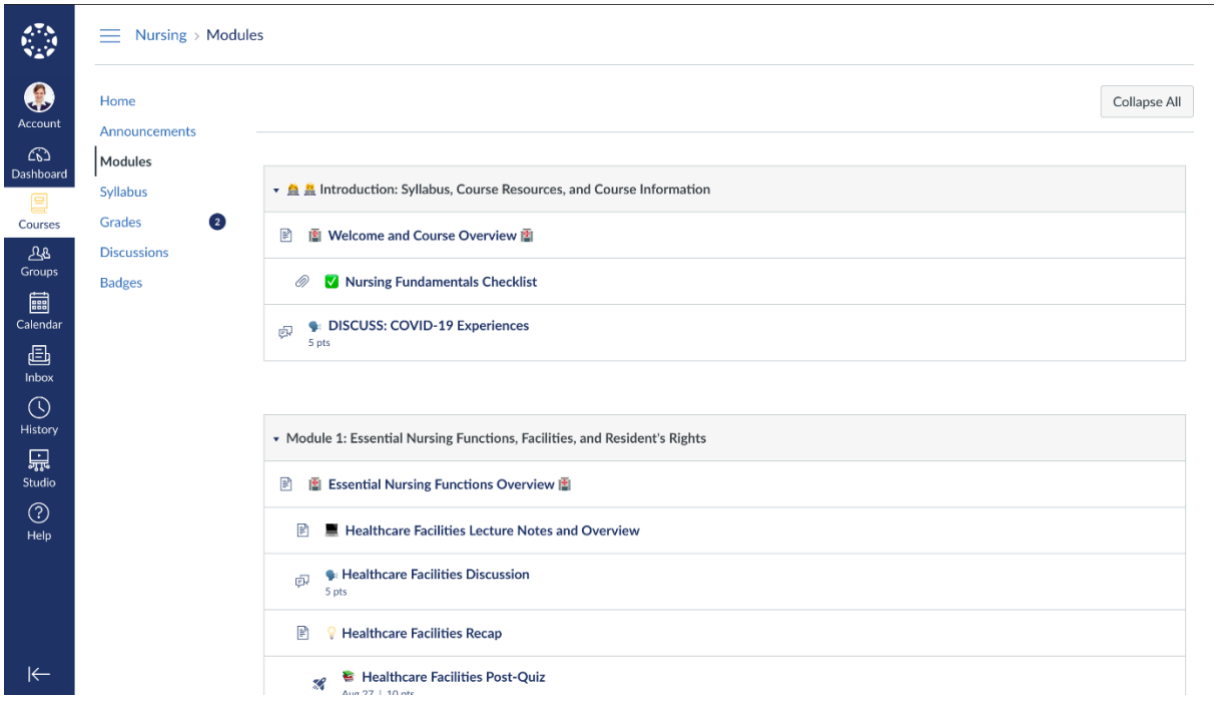
Canvas LMS is a cloud-based, open-source Learning Management System with advanced LMS functionalities. It can be easily accessed from any device, from anywhere, anytime. Through open APIs and adherence to LTI standards, Canvas LMS provides easy integration with a network of 600+ education technology partners including Google Classroom, Microsoft Teams, Zoom, and Adobe. It allows administrators and faculty to innovate and customise courses while giving students a personalized and engaging experience.




Screenshot 6: Canvas



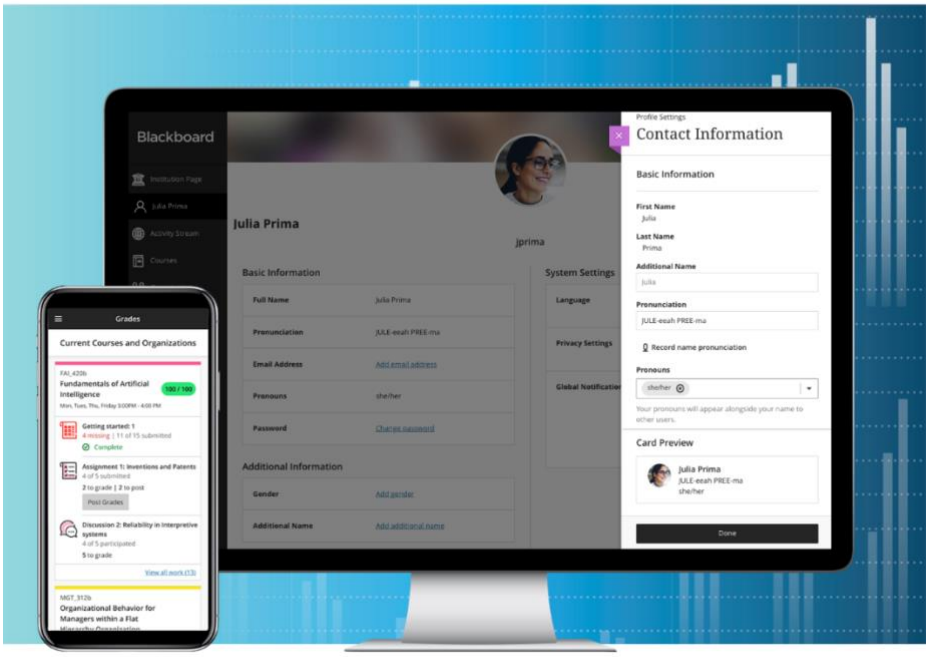

Screenshot 7: Canvas



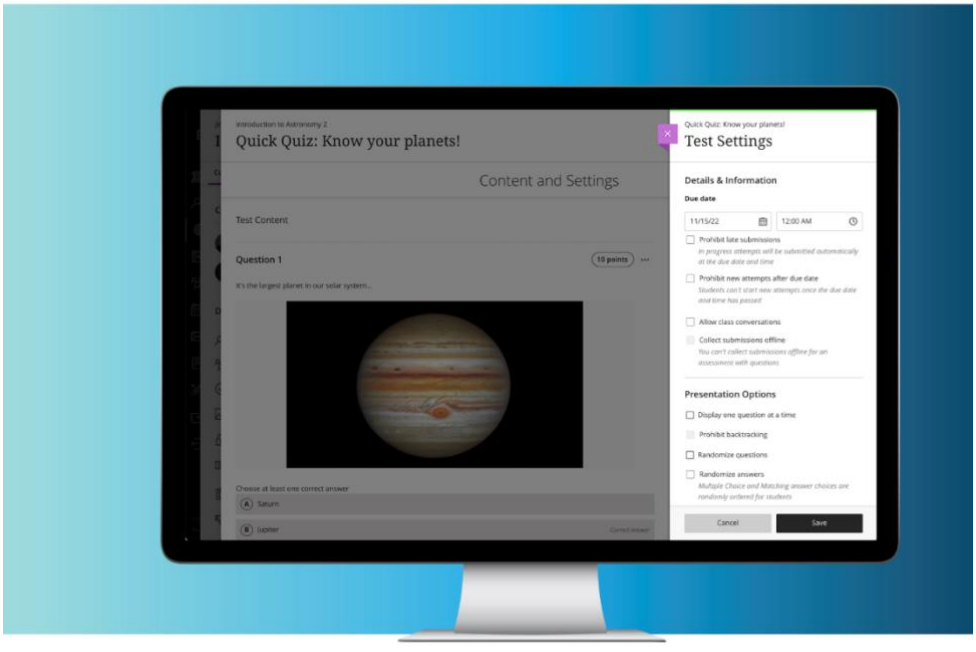

Screenshot 8: Canvas

Blackboard Learn - Blackboard Learn learning management system (LMS)

Blackboard Learn is and open-source cloud-based Learning Management System that provides built-in course construction and management tools to help deliver teaching and learning experiences and system reliability to keep learners engaged and on track. It also provides easy student registration, enrolment and payment for courses.



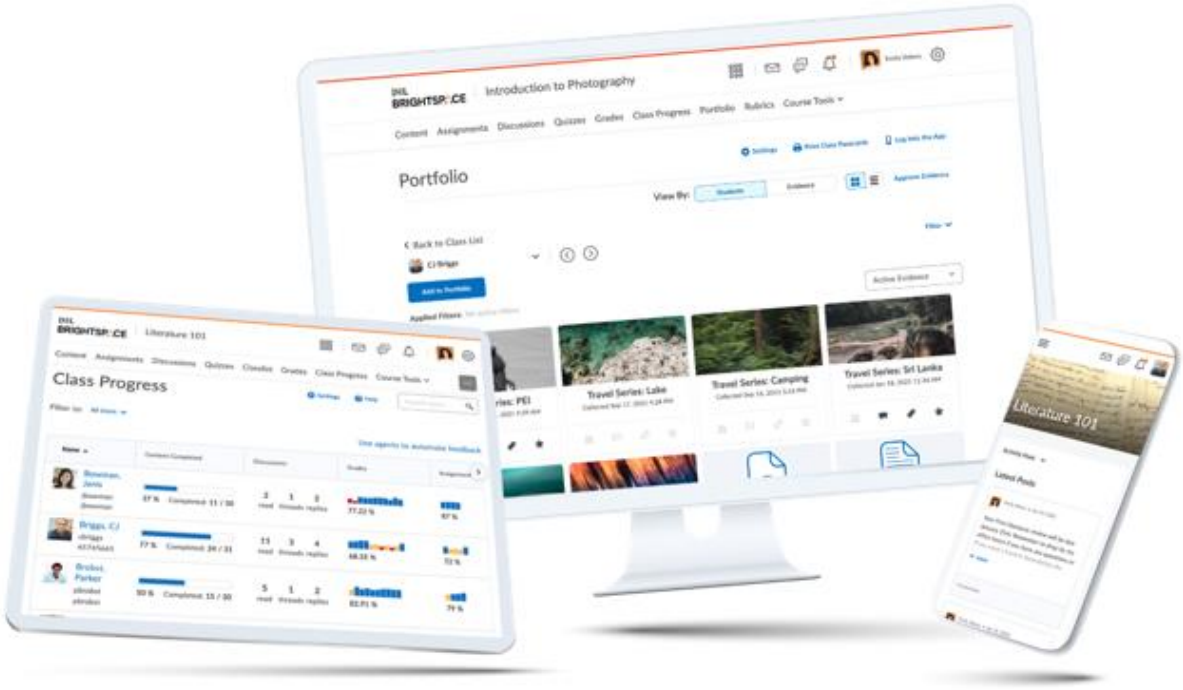

Screenshot 9: Blackboard Learn




Screenshot 10: Blackboard Learn

D2L Brightspace - Brightspace Learning Management System | LMS Platform | D2L

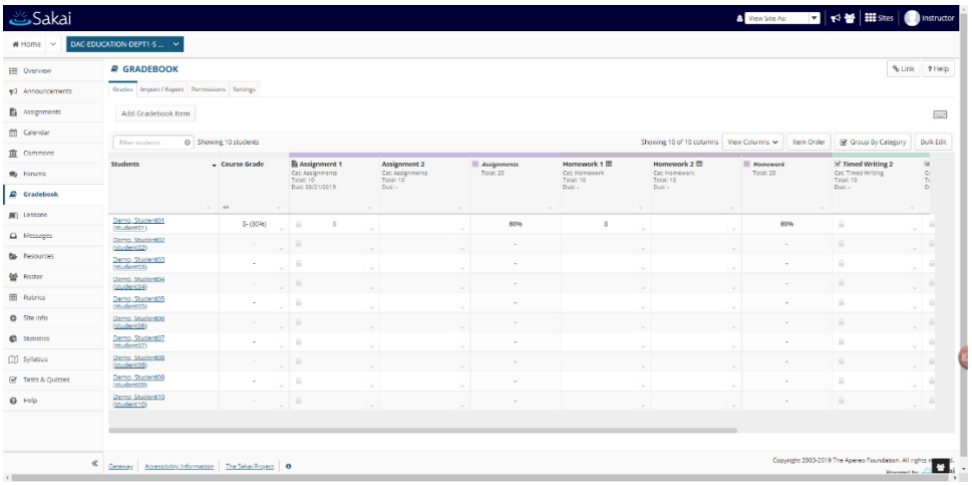
Brightspace by D2L combines research-driven tools, services, and expert support to deliver a high-quality teaching and learning experience—all in one convenient package. Save time with reliable learning tools in one centralized hub—course materials, videos, tests, and more. Access the intuitive, mobile-friendly cloud-based platform on any device to work at your own pace. Monitor student progress with easily digestible analytics dashboards.



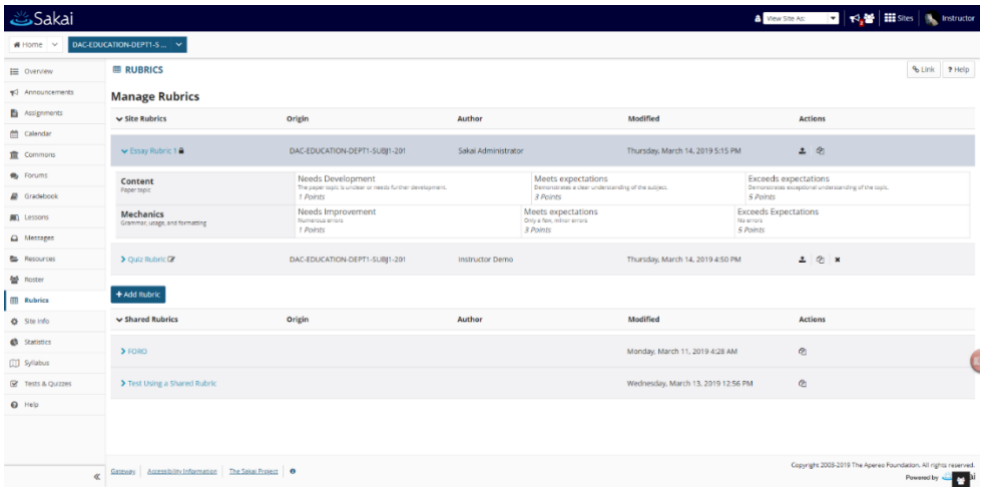

Screenshot 11: D2L Brightspace

Sakai - Sakai Learning Management System | Sakai LMS

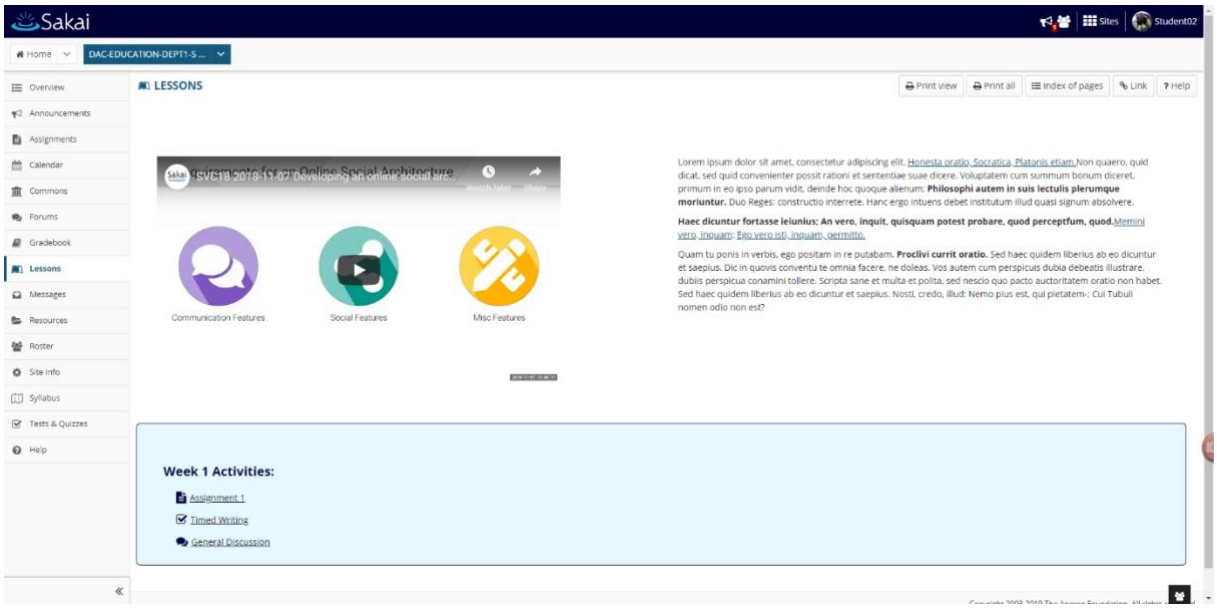
The Sakai Environment provides a flexible and feature-rich environment for teaching, learning, research and other collaboration. As an open-source software suite developed by its adopter community, Sakai continually evolves in step with the needs of the students, faculty members and organisations it serves.



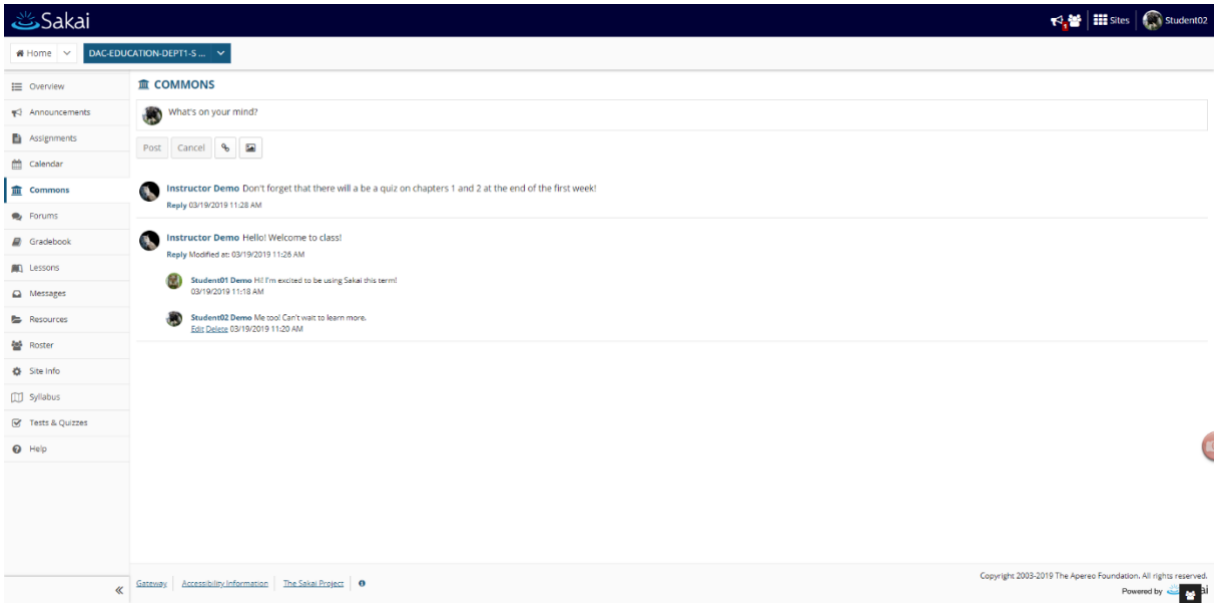

Screenshot 12: Sakai Learning Management System




Screenshot 13: Sakai Learning Management System



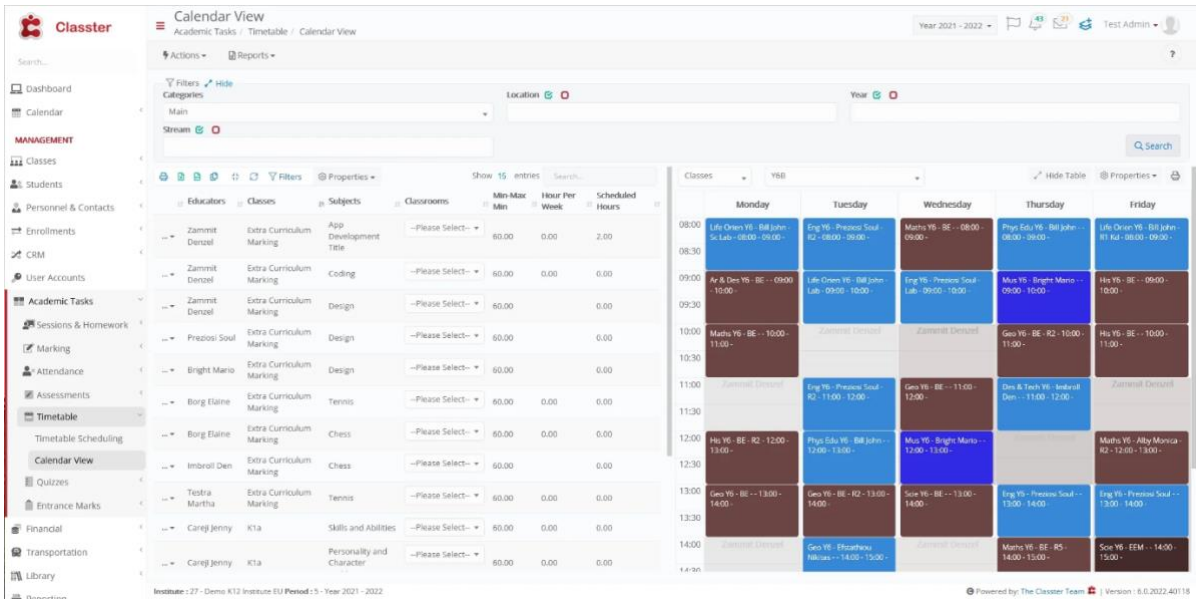

Screenshot 14: Sakai Learning Management System



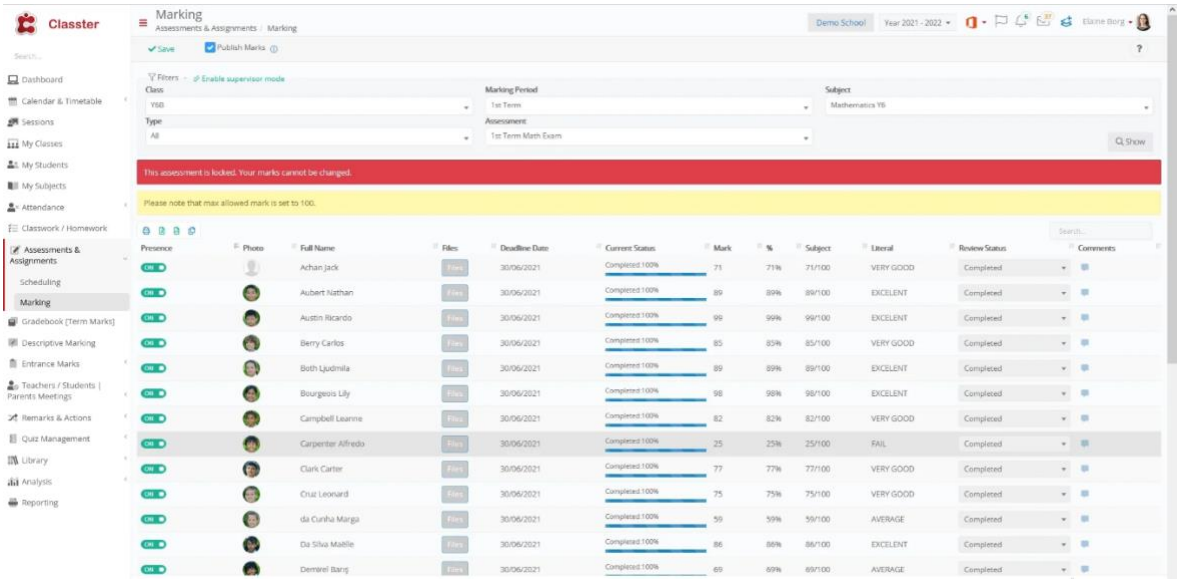

Screenshot 15: Sakai Learning Management System

Classter - School Learning & Student Information Management - Classter

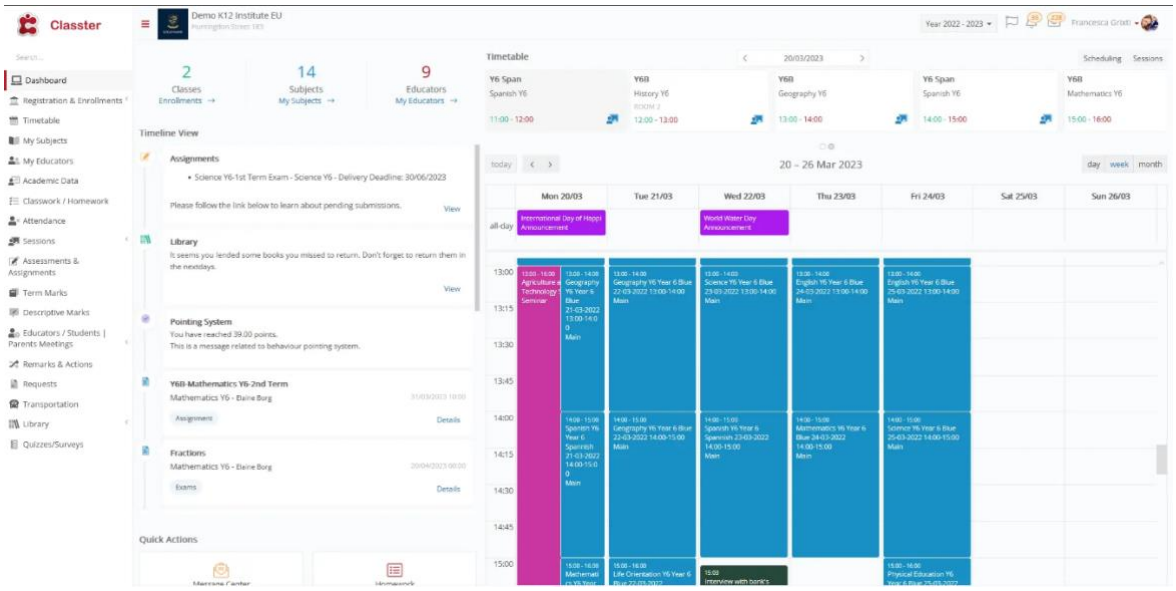
With Classter you will have access to a comprehensive suite of modules, including Admissions, Billing, CRM, LMS, SIS, Transportation, Library management, and Alumni management, all integrated into one simple and intuitive platform. It is able to provide an easy-to-use, reliable, secure, and efficient way for educational institutions to manage their processes and administration from enrolment to alumni. It is also integrated with over 40 most popular tools in education, so you can easily incorporate it into your existing workflow.



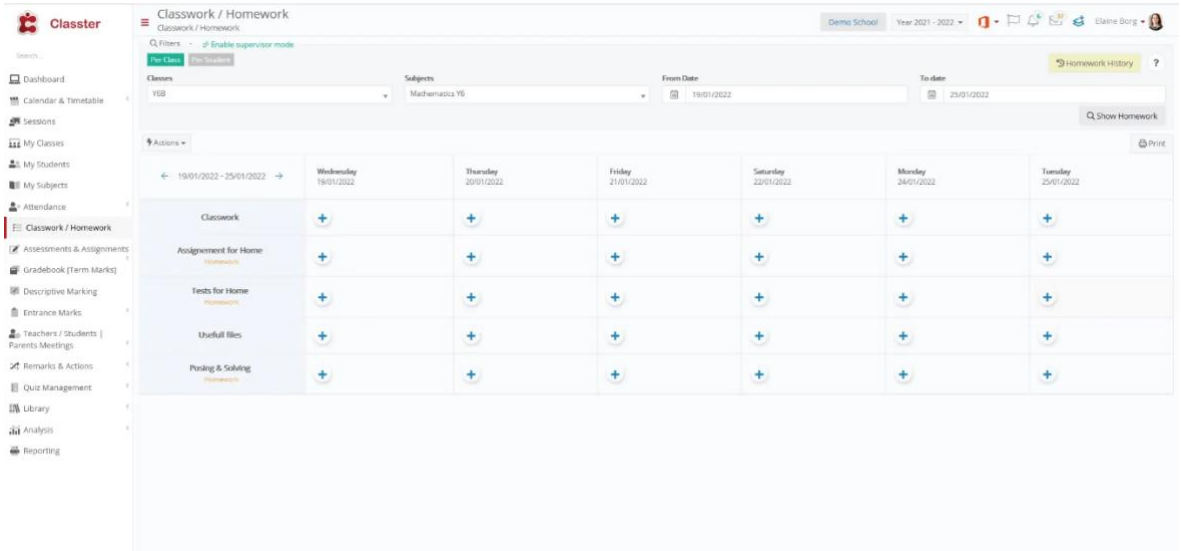

Screenshot 16: Classter




Screenshot 17: Classter




Screenshot 18: Classter

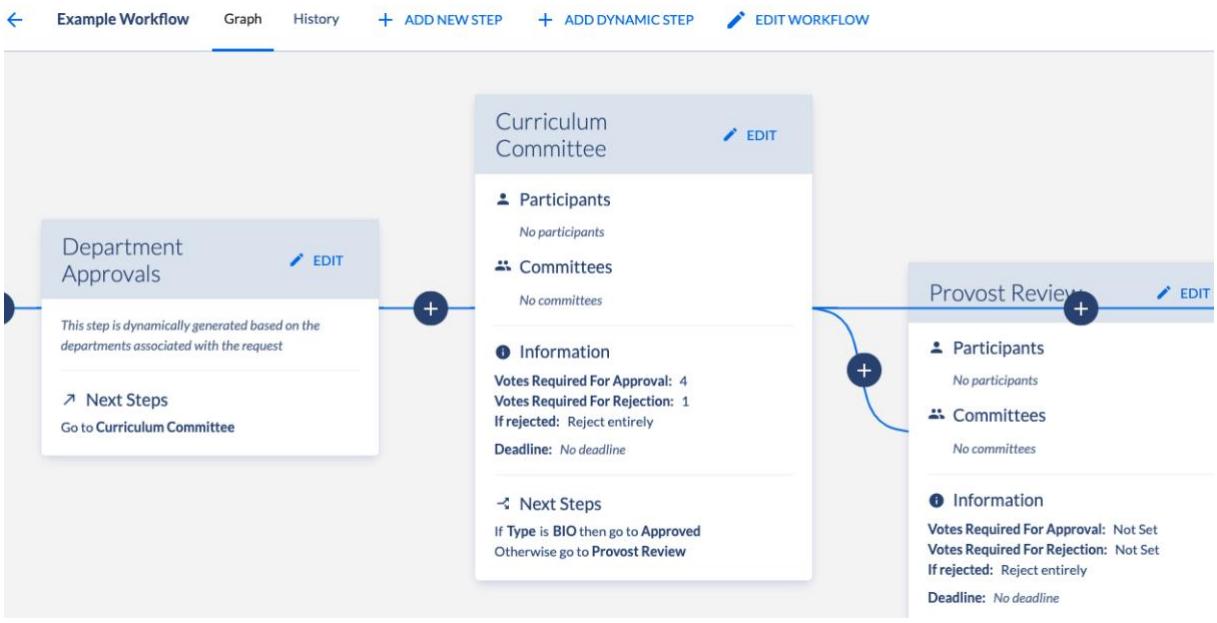



Screenshot 19: Classter

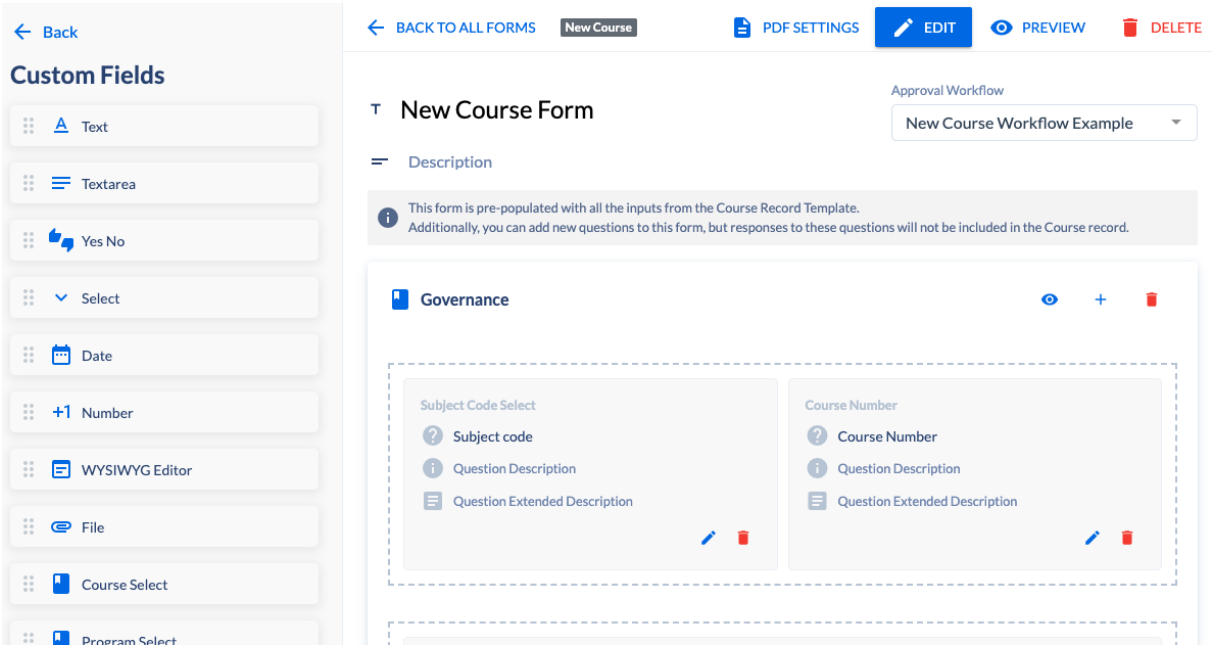
Coursedog - Curriculum and Catalog Management | Coursedog

Coursedog is a curriculum management platform that integrates academic and event scheduling, curriculum and catalogue management, and course demand projections and analytics. Using a single, bi-directional integration with SIS and adopting work scheduling software features, Coursedog executes student-centric, cost-efficient schedules while integrating academic scheduling. This end-to-end solution delivers actionable course demand projections that support operational excellence. Coursedog integrates with communication platforms as well as SSO providers like SAML, Shibboleth, and CAS.


Screenshot 20: Coursedog



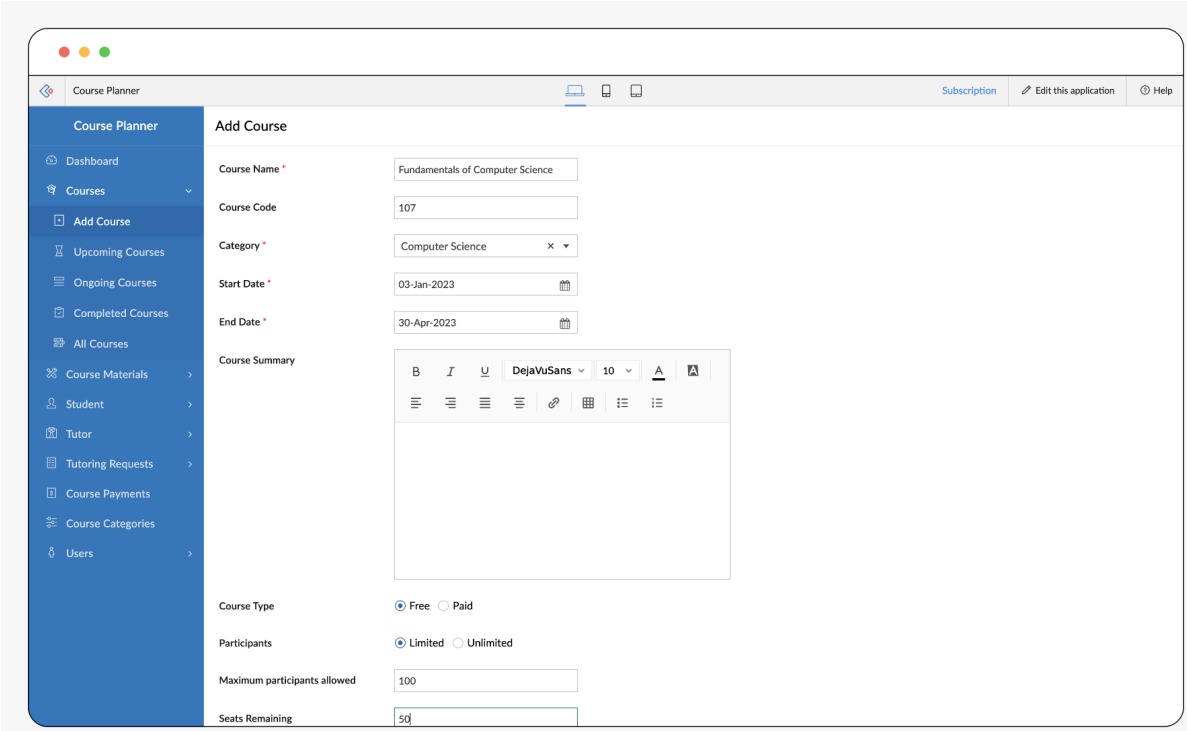

Screenshot 21: Coursedog



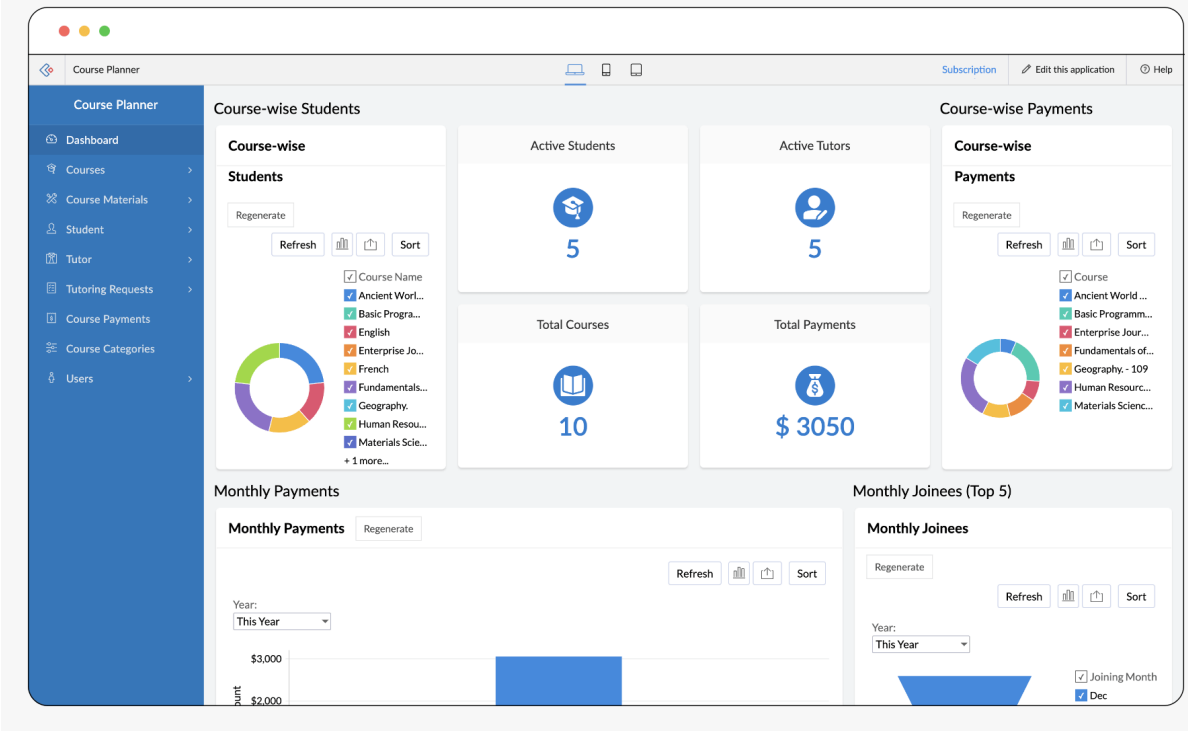

Screenshot 22: Coursedog

Zoho Creator - Course Planner - Curriculum Management Mapping Software | Zoho Creator

Manage all the courses you offer, and the details of your students and tutors. See who is in charge of which course and follow payments until they are credited. Give a separate area for students and tutors to manage their personal details, their current and upcoming courses, and payments. Split up your students and tutors as either the current batch of those pending assignment. Enable e-mail notifications for course updates and keep students and tutors in the know.




Screenshot 23: Zoho Creator - Course Planner

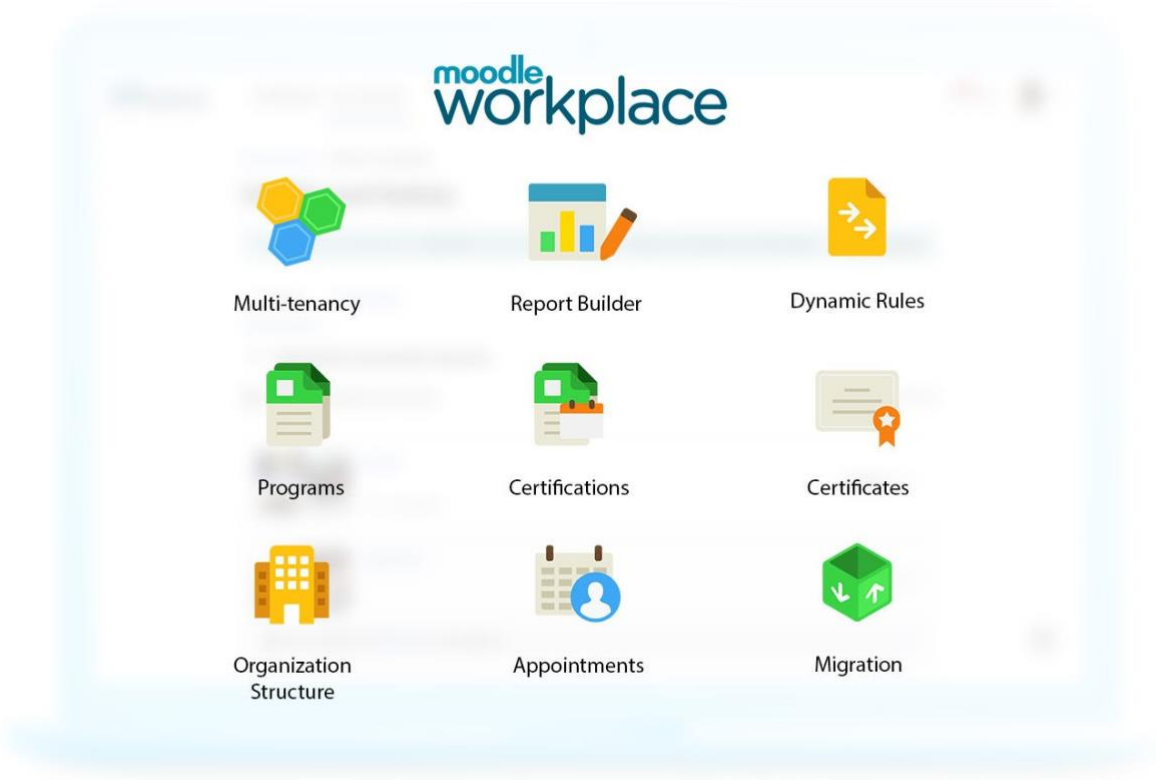



Screenshot 24: Zoho Creator - Course Planner

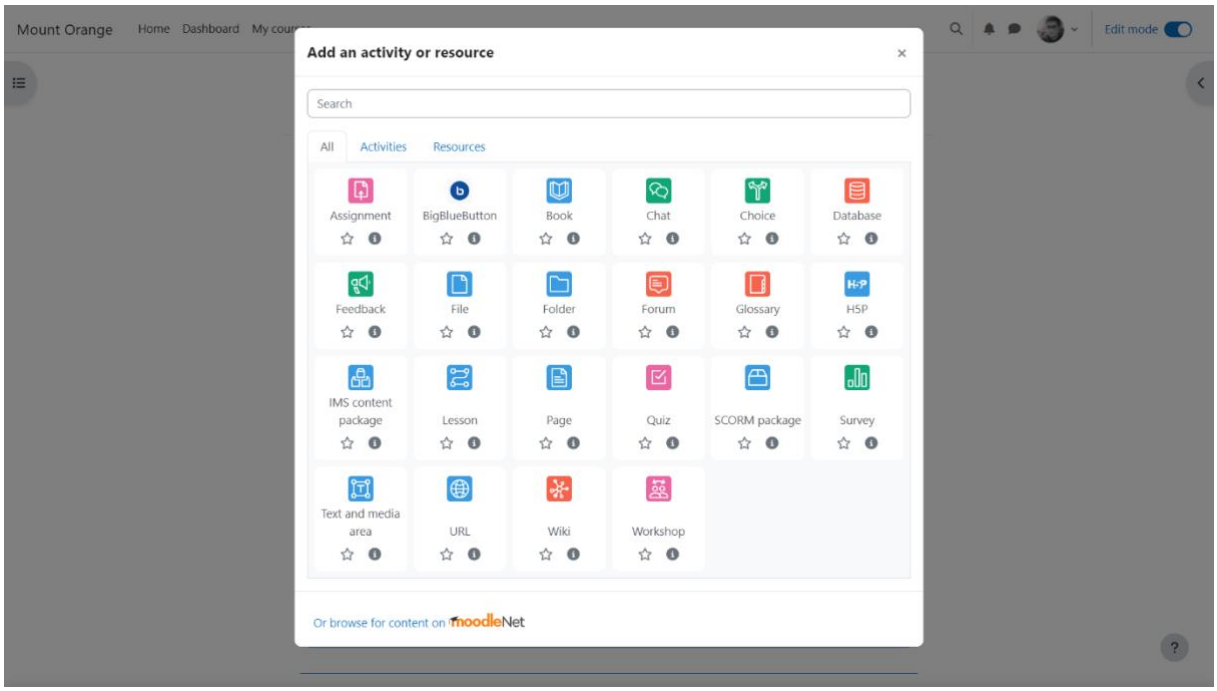
### 5.4.2 Open Licence Solutions

Moodle (A brief reference) -

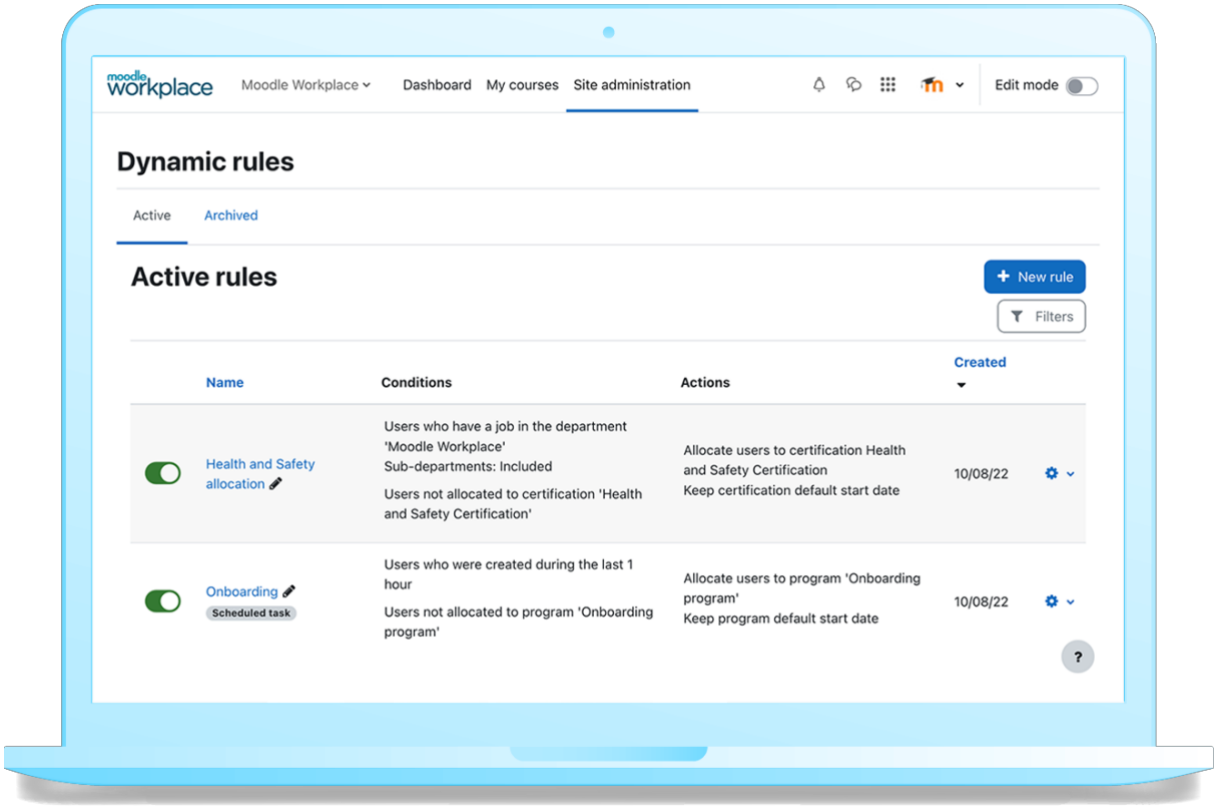
Moodle, though more popularly known as a learning management platform, is also an open-source curriculum software. The Moodle system can be expanded to function as a hub for academic collaboration and curriculum management. Within Moodle, you can create and organise courses based on your curriculum and incorporate educational standards. Moodle can also be configured to generate data on student access and performance on the site. More info about Moodle will be provided at the end of this chapter.




Screenshot 25: Moodle



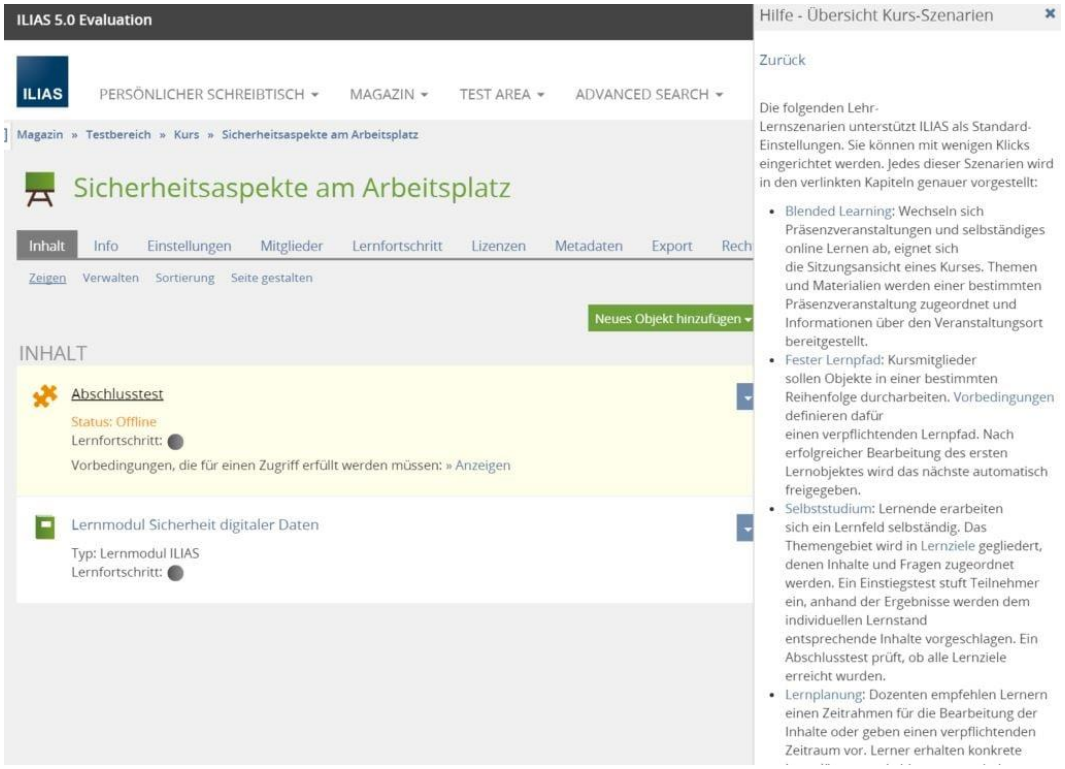

Screenshot 26: Moodle




Screenshot 27: Moodle

Ilias - ilias.de

Ilias is a powerful open-source Learning Management System for developing and realizing web-based e-learning. The software was developed to reduce the costs of using new media in education and further training to ensure the maximum level of customer influence in the implementation of the software.




Screenshot 28: Ilias

Open eClass

Open eClass is an open-source Learning Management System designed to provide a platform for online teaching and learning within educational institutions. It features a user-friendly interface, making it accessible for both educators and learners to navigate course materials, assignments, and communication tools. Open eClass offers various features such as course management, collaboration tools, multimedia integration, and assessment support, aiming to provide educators with the flexibility to create engaging and interactive courses. Additionally, it includes communication features like announcements, messaging, and notifications to foster seamless interaction among educators and learners. The platform also prioritizes data security and user privacy, aligning with essential standards and regulations.

However, it is worth noting that in comparison to widely recognised LMS platforms like Moodle, Open eClass may not possess the same extensive user community and ecosystem of plugins and integrations. This limitation can affect its adaptability and compatibility with various educational environments. Consequently, further comparisons with other available Learning Management System options may be constrained by these factors, particularly when considering Moodle's broader adoption and comprehensive support network.

In summary, Open eClass modestly positions itself as an open-source LMS, catering to the needs of educational institutions. While it offers several commendable features, its comparative limitations in terms of user community and integration support warrant a measured assessment when considering it as an LMS option. Nonetheless, it remains a viable choice for institutions seeking a tailored, cost-effective solution for their unique educational needs.

### 5.4.3 Overall Assessment

The assessment is summarised in table 17/18.

Table 17: Overview of DCM system assessment

| Assessment Criteria | Powerschool | Atlas | Schoolinsight | Moodle | Canvas | Blackboard Learn |
|---|---|---|---|---|---|---|
| **Features** | | Hard to keep up with "heavy-duty" requirements | Supplemental features cost extra | Wide range of easy to use features | Customi-sable features | Small variety of features |
| **User Friendly** | Difficult to new users | Easy interface | Easy to navigate | Many plugins and add-on tools to make it user friendly | Too complex | Room for visual improve-ment |
| **Flexibility** | Way too complex | | | Easy course design to match each user | Flexible course design | Not a lot of design flexibility |
| **Integration** | Reported 3rdparty integration issues | | | Easy process adjustment between software | Efficient, easy to setup | Bad syllabus integration system |
| **Technical Customer Support** | Difficult to reach | | High average waiting time | | Support sometimes inex-perienced | Great technical support team |
| **Cost / Price** | €€€€ | €€€ | €€ | Free version available | €€€ | €€ |
| **User Feedback** | 4,2/5 | 3,3/5 | 4,1/5 | 4,5/5 | 4,4/5 | 3,9/5 |
| **Up to date** | Custom pages needed | | | | Great up-to-date feedback | Not as up to date as other platforms |
| **Data Security** | Security user groups/ access a bit confusing | | | | Constant password change required | |

Table 18: Overview of DCM system assessment (cont.)

| Assessment Criteria | Brightspace | Sakai | Classter | Coursedog | Zoho | Ilias |
|---|---|---|---|---|---|---|
| **Features** | Some Features not fully | Wide variety but | | | | Allows a lot of possibilities |

| | | | | | | |
|---|---|---|---|---|---|---|
| | developed when deployed | simple features | | | | |
| **User Friendly** | Difficult to navigate | Little overwhelming to new users | Interface is not very user-friendly | | Easy to learn | Too complex, requires a lot of training to fully use all its features |
| **Flexibility** | Easily customisable | Flexible design | | | Limited customi-sation | Open Source |
| **Integration** | Challenging integration | Integration with only basic software | Tricky and challen-ging integration | | | |
| **Technical Customer Support** | Great support feedback | | | | Slow to respond | |
| **Cost / Price** | €€ | € | € | €€€€ | €€€ | Free version available |
| **User Feedback** | 4,3/5 | 3,7/5 | 4,3/5 | Lack of online reviews | 4,2/5 | 4,6/5 |
| **Up to date** | Continuous updates | | | | Some features not up-to-date | |
| **Data Security** | | | | | | |

*All information gathered from online user reviews and user ratings on www.g2.com, www.research.com, www.sourceforge.net, www.gartner.com, www.getapp.com, www.slashdot.org.

Most of the Curriculum Management Systems listed above offer a wide variety of features, with Moodle, Canvas, Sakai, Brightspace and Ilias being the best picks based on the CyberSecPro needs and their own flexibility.

Powerschool, Blackboard Learn, Classter, Ilias and Zoho Creator, although being highly customisable, are also reported by reviewers as difficult to work on. Their interface complexity and learning difficulties for new users constitute a major downside comparing to the rest.

There have also been reports of non-efficient and challenging integration systems for Powerschool, Sakai, Blackboard Learn, and Brightspace, with issues in integrating with 3rd party platforms.

When comparing Open eClass and Moodle, Moodle emerges as a robust choice for educational institutions, thanks to several key strengths. Moodle boasts an extensive and thriving user community, offering a vast array of resources and support forums. Its rich ecosystem of plugins and integrations provides exceptional customisation and extensibility options, catering to diverse educational needs. Additionally, Moodle's well-established track record in the eLearning industry makes it a trusted choice for numerous educational institutions and organizations worldwide. While Open eClass has its merits, such as a user-friendly interface and basic features for online teaching and learning, it faces limitations. Open eClass's relatively small user community can result in limited resources and potentially slower issue resolution. Furthermore, it may encounter challenges in integrating with other systems and tools due to its smaller ecosystem of plugins and integrations. Open eClass's recognition and adoption may also fall short compared to Moodle, impacting its ability to gain institutional support and widespread usage. In conclusion, Moodle's extensive user community, versatile plugin ecosystem, and established

reputation position it as a powerful and reliable Learning Management System for educational institutions.

Moodle can be listed as the best option to fit the mentioned criteria. Being open-source and completely free, as well as its wide range of features and variety of plugins and add-on tools that can be used, places it at the top of the list to be chosen as the Curriculum Management System.

## 5.5 Moodle: An extensive reference of its capabilities

The field of education has undergone substantial change in today's fast-paced and technologically driven environment. Learning Management Systems (LMS) have become vital tools for educational institutions, organisations, and individuals wanting to improve their learning experience with the introduction of e-learning and online education. Among the different LMS platforms available, Moodle is one of the most extensively used and well-regarded systems.

Moodle, which stands for "Modular Object-Oriented Dynamic Learning Environment," is an open-source learning management system that helps educators to successfully create, organise, and deliver online courses. Moodle, created by Martin Dougiamas in 2002, has grown in popularity because to its flexibility, large feature set, and active community support. It is used by millions of educators and learners across the globe, spanning diverse sectors such as K-12 education, higher education, corporate training, and non-profit organisations. [54]

Moodle's open-source nature is one of its primary advantages. Because Moodle is an open-source platform, its source code is freely available for anybody to use, alter, and share. This transparency encourages a collaborative environment, enabling developers, instructors, and administrators to contribute to the organisation's ongoing improvement. As a result, Moodle has a thriving user community that is constantly improving its functionality, security, and compatibility [55].

Moodle offers a comprehensive set of features that cater to the diverse needs of both instructors and learners. Its intuitive interface allows educators to create engaging and interactive courses by incorporating multimedia content, quizzes, assignments, and discussion forums. Moreover, Moodle supports various assessment methods, including online quizzes, grading tools, and peer review systems, providing educators with the flexibility to evaluate student progress efficiently [56].

For learners, Moodle provides a user-friendly environment that promotes active engagement and knowledge retention. Learners can use a centralized online platform to access course materials, participate in conversations, communicate with peers, and submit assignments. Moodle also provides customised learning paths, allowing students to progress at their own speed and access resources tailored to their specific needs [57].

Another notable feature of Moodle is its extensive integration capabilities. The platform supports interoperability standards such as SCORM (Sharable Content Object Reference Model) and LTI (Learning Tools Interoperability), enabling seamless integration with external tools and systems. This interoperability empowers institutions to leverage their existing technology infrastructure, such as content repositories, student information systems, and virtual classrooms, while providing a unified learning experience [58].

Furthermore, Moodle's flexibility extends beyond its core functionalities. The platform supports a wide range of plugins and extensions, allowing institutions to customise and extend Moodle's capabilities according to their specific requirements. Whether it's integrating with third-party tools, adding new functionalities, or creating unique learning experiences, Moodle's modular architecture ensures scalability and adaptability [59].

In conclusion, Moodle has emerged as a leading Learning Management System, renowned for its open-source nature, rich feature set, and active community. With its user-friendly interface, comprehensive tools, and customisation options, Moodle empowers educators and learners to create and engage in dynamic online learning experiences. As education continues to evolve in the digital age, Moodle remains a powerful platform that embraces innovation and caters to the ever-changing needs of modern learners.

### 5.5.1 Characteristics of Moodle

The most important characteristics of Moodle are as follows [57] [59] [60] [61]:

1. Open-Source and Customisability: The open-source nature of Moodle is a big advantage because it offers institutions and organisations a great level of flexibility and customisability. Because Moodle is open-source, the source code is publicly available, allowing organisations to alter and enhance it to meet their specific needs. Customising the user interface, creating new features, integrating external systems, and adjusting the platform to meet branding rules are all part of the process. The open nature of Moodle empowers institutions to create a tailored and unique learning environment that suits their educational objectives.
2. Large and Active Community: One of the key strengths of Moodle is its large and active community of users, developers, and contributors worldwide. This vibrant community actively contributes to the platform's development, support, and improvement. The community provides a wealth of resources, including forums, documentation, user guides, tutorials, and plugins. Users can seek assistance, share best practices, and exchange ideas with peers who have extensive experience using Moodle. The active community ensures that Moodle remains current, responsive to user needs, and continuously evolves to meet emerging trends and educational requirements.
3. Cost-Effective Solution: Moodle offers a cost-effective solution for organisations and educational institutions. As an open-source platform, Moodle eliminates the need for costly licensing fees typically associated with proprietary LMS solutions. Institutions can leverage Moodle's features and functionalities without incurring significant upfront expenses, making it an attractive option for those with limited budgets. The cost savings can be allocated towards further customisation, training, support, or additional educational initiatives, maximising the value derived from the investment in Moodle.
4. Robust Features and Functionality: Moodle provides a comprehensive set of features and functionalities that cater to various aspects of online learning. It offers tools for content creation, course management, assessments, collaboration, grading, reporting, and more. These features empower instructors to design engaging and interactive learning experiences. Whether it's creating multimedia-rich content, setting up discussion forums, conducting quizzes and assignments, or tracking learner progress, Moodle provides a robust and versatile learning environment that supports diverse pedagogical approaches.
5. Flexibility in Content Creation: Moodle offers instructors flexibility in creating diverse and interactive learning content. The platform supports various formats, including text, images, videos, audio, quizzes, assignments, and interactive activities. This flexibility allows instructors to design engaging and personalized learning experiences that cater to different learning styles and objectives. Instructors can incorporate multimedia elements, interactive exercises, and real-world scenarios, fostering active participation and knowledge retention among learners.
6. Community Engagement and Collaboration: Moodle emphasizes collaboration and communication among learners through features such as discussion forums, messaging systems, wikis, and group activities. These tools promote interaction and engagement, creating a sense of community within the online learning environment. Learners can actively participate in discussions, share ideas, collaborate on projects, and provide feedback to their peers. The emphasis on community engagement fosters a collaborative learning culture and enhances the overall learning experience.
7. Multilingual and Localisation Support: Moodle recognises the importance of catering to diverse learner populations and offers robust multilingual and localisation support. It supports a wide range of languages, allowing institutions to deliver courses in different languages to reach a global audience. Moodle's localisation capabilities enable institutions to adapt the platform to local language preferences, cultural norms, and educational requirements. This localisation support ensures that learners from different regions can access content and interact with the platform in their preferred language, fostering inclusivity and accessibility.

8. Constant Development and Upgrades: Moodle follows a continuous development cycle, regularly releasing updates and new features to address security, performance, and usability improvements. The development team actively listens to user feedback, incorporates industry best practices, and stays ahead of emerging trends in education and technology. Regular updates and upgrades ensure that Moodle remains relevant, reliable, and aligned with evolving educational needs. Institutions can benefit from these enhancements to deliver a cutting-edge learning experience to their learners.
9. Integration Capabilities: Moodle offers extensive integration capabilities, enabling seamless interoperability with external systems and tools. It supports integration with student information systems (SIS), authentication systems, content repositories, video conferencing platforms, learning analytics tools, and more. These integrations streamline workflows, reduce duplication of efforts, and enhance the overall learning experience. Institutions can leverage existing systems and tools within their ecosystem, creating a cohesive and efficient learning environment for both instructors and learners.
10. Scalability and Community Support: Moodle has proven scalability, capable of supporting small organisations as well as large institutions with thousands of users. Its robust architecture and community-driven development ensure that Moodle performs well and remains stable, even under heavy usage. The active community provides valuable support, knowledge sharing, and best practices for scaling Moodle deployments. Organizations can rely on the collective expertise of the community to optimize performance, ensure reliability, and address scalability challenges when implementing Moodle on a larger scale.

In conclusion, Moodle's open-source nature, extensive community support, cost-effectiveness, robust features and functionality, flexibility in content creation, emphasis on collaboration, multilingual support, constant development and upgrades, integration capabilities, and scalability make it a compelling choice for institutions and organisations seeking a comprehensive and adaptable learning management system.

### 5.5.2 Moodle Assessment

This section presents how Moodle surpasses other LMS/CMS [62] [63], analysing the aforementioned criteria.

1. Features and Functionality: Moodle offers an extensive range of features and functionalities that set it apart from other LMS/CMS platforms. It provides a comprehensive suite of tools for content management, course creation, assessments, collaborative activities, communication, and grading. Administrators have the flexibility to create engaging and interactive courses using various multimedia formats. Additionally, Moodle supports a wide range of question types for assessments and offers robust reporting capabilities to track learner progress and performance. Its modular design allows for the integration of additional features through plugins, providing endless possibilities for customisation and meeting specific organisational needs.
2. User-Friendliness: Moodle excels in providing a user-friendly interface that promotes ease of use for both administrators and learners. Its intuitive navigation and well-organised menus make it effortless to navigate through the system. Administrators can easily manage courses, enrol learners, and set permissions with a few simple clicks. Learners, on the other hand, can access their courses, view resources, submit assignments, and participate in discussions with ease. Moodle's clean design and user-friendly interface contribute to a positive learning experience and promote learner engagement.
3. Scalability and Flexibility: Moodle is designed to scale seamlessly, making it suitable for organisations of all sizes. Whether you have a small team or a large-scale institution with thousands of users, Moodle can accommodate your needs. It supports multiple courses and learners simultaneously, allowing for efficient management of diverse learning environments. Furthermore, Moodle offers flexibility in terms of learning modalities, supporting online, blended, and self-paced learning. This adaptability ensures that Moodle can cater to various

educational needs and teaching methods, making it an ideal choice for organisations with evolving requirements.

4. Integration Capabilities: Moodle stands out with its robust integration capabilities, allowing for seamless integration with external systems, tools, and services. It offers standard integration options for popular tools such as video conferencing platforms, content authoring tools, student information systems, and learning analytics tools. Furthermore, Moodle supports industry standards like Learning Tools Interoperability (LTI) and SCORM, enabling easy integration with a wide range of third-party applications and content. This integration capability enhances the overall learning experience by providing a unified and cohesive learning ecosystem.
5. Customisation and Branding: Moodle provides extensive customisation options, empowering organisations to create a unique and branded learning environment. Administrators can customise the appearance of Moodle to match their organisation's branding and visual identity. They can tailor course templates, configure layout options, and add branding elements to create a consistent and personalized learning experience. This level of customisation ensures that Moodle aligns with the organisation's specific requirements and promotes a sense of ownership and familiarity among learners.
6. Technical Support and Reliability: Moodle benefits from a large and active community of users and developers, contributing to its robust technical support and reliability. Administrators and educators have access to an extensive knowledge base, forums, user communities, and documentation to help them navigate the system effectively. The Moodle community actively addresses queries, shares best practices, and offers solutions to technical challenges. Furthermore, Moodle releases regular updates, bug fixes, and security patches to ensure the platform's stability, reliability, and data security.
7. Cost and Value: Moodle's open-source nature makes it a cost-effective solution compared to proprietary LMS/CMS platforms. Organizations can benefit from significant cost savings, as there are no licensing fees associated with Moodle itself. Additionally, Moodle's extensibility and customisation options allow organisations to tailor the platform to their specific needs without incurring additional costs. The availability of a strong community and support network also adds value by providing ongoing support, resources, and continuous development.
8. User Feedback and Reviews: Moodle boasts a large and vibrant user community, contributing to an extensive pool of feedback, reviews, and best practices. Administrators and educators can leverage this collective knowledge to enhance their Moodle experience, gain insights, and access valuable resources. The user community actively shares experiences, tips, and innovative approaches, enabling continuous improvement and fostering collaboration among users. Learning from the experiences and feedback of others ensures that organisations can optimize their Moodle implementation and maximise its benefits.
9. Future Readiness and Innovation: Moodle has a proven track record of continuous development and innovation, positioning it as a future-ready LMS/CMS platform. The Moodle team consistently updates the platform to incorporate emerging trends and technologies in the education sector. This includes advancements such as mobile learning, gamification, adaptive learning, learning analytics, and integration with emerging technologies like virtual reality and artificial intelligence. By embracing innovation, Moodle ensures that organisations can leverage cutting-edge tools and approaches to deliver effective and engaging learning experiences.
10. Data Encryption: Data security is a top priority for Moodle, and it employs robust data encryption measures to ensure the secure transmission and storage of sensitive information. Moodle incorporates encryption through the use of Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols. This encryption safeguards user credentials, personal information, and other sensitive data exchanged between users and the Moodle system, protecting it from unauthorised access or interception. By implementing SSL/TLS, Moodle maintains a secure learning environment and ensures the privacy and confidentiality of user data.

Overall, Moodle's extensive features, user-friendliness, scalability, integration capabilities, customisation options, strong support network, cost-effectiveness, user community, commitment to

innovation, and data security measures make it the ideal choice for organisations and educational institutions seeking a comprehensive and reliable LMS/CMS platform.

### 5.5.3 Moodle Customisation Using Plugins

Moodle, as an open-source Learning Management System (LMS), offers a wide range of features and functionalities to support online learning. One of the strengths of Moodle lies in its extensive plugin ecosystem, which enhances the platform's core functionality and provides additional specialized tools to meet specific educational needs [64]

Content Management: Moodle offers various plugins to facilitate content management. Plugins like the Book module allow instructors to create structured content in a book-like format, while the Lesson module enables the creation of interactive lessons with branching scenarios. Additionally, the H5P plugin allows for the creation of rich interactive content, such as quizzes, presentations, and interactive videos, directly within Moodle.

Assessment and Quiz Tools: Moodle provides a comprehensive set of assessment and quiz tools to evaluate learners' progress and knowledge. The Quiz module offers a range of question types, including multiple-choice, short answer, and essay questions. Plugins like the Questionnaire module enable the creation of surveys and feedback forms, while the Feedback module allows instructors to collect feedback from learners to improve course materials.

Communication and Collaboration: Moodle offers plugins to facilitate communication and collaboration among learners and instructors. The Forum module enables discussions and knowledge sharing in threaded discussion forums. The Chat module provides real-time communication, allowing learners to interact synchronously. Plugins like BigBlueButton and Zoom integrate video conferencing capabilities into Moodle, facilitating virtual classrooms and online meetings.

Reporting and Analytics: Moodle includes built-in reporting capabilities, but additional plugins extend its analytics capabilities. Plugins like the Configurable Reports module provide advanced reporting features, allowing administrators and instructors to generate custom reports based on various data points. Learning Analytics plugins, such as Learning Analytics Recommendations and Predictive Analytics, leverage data analysis techniques to provide insights into learners' performance and personalize learning experiences.

Gamification and Engagement: To enhance learner engagement, Moodle offers plugins that incorporate gamification elements. Plugins like Level Up! provide a gamified experience, where learners earn experience points, badges, and levels as they progress through courses. Interactive video plugins, such as H5P Interactive Video, enable the creation of interactive videos with embedded quizzes, branching scenarios, and hotspots, making learning more interactive and engaging.

Integration with External Tools and Systems: Moodle supports integration with external tools and systems through plugins, enabling a seamless learning ecosystem. Plugins like the LTI (Learning Tools Interoperability) module allow for integration with external learning tools, such as content authoring tools, e-portfolios, and virtual lab environments. Plugins like the LDAP (Lightweight Directory Access Protocol) Authentication enable seamless integration with existing authentication systems, simplifying user management and access control.

Mobile Learning: Moodle offers mobile learning capabilities through plugins and responsive design. The Moodle app, available for iOS and Android, provides a mobile-friendly interface, enabling learners to access course materials, participate in activities, and receive notifications on their mobile devices. Plugins like the Mobile app service plugin allow for customisation and integration of additional mobile features, such as push notifications and offline content access.

Accessibility and Universal Design: Moodle emphasizes accessibility and provides plugins to enhance the learning experience for learners with diverse needs. Plugins like the Accessibility block offer accessibility tools and features, such as font resizing, colour contrast adjustment, and screen reader compatibility.

Social Learning and Networking: Moodle promotes social learning and networking through plugins that facilitate communication and collaboration. The Socialwall plugin creates a social media-like environment within Moodle, where learners can share updates, resources, and engage in discussions. Plugins like the User Tours provide guided tours and walkthroughs, helping learners navigate the Moodle platform and discover its features.

The extensive range of Moodle plugins demonstrates the platform's versatility and adaptability to cater to various educational requirements. Institutions and organisations can leverage these plugins to customise their Moodle instance, aligning it with their specific needs and providing a tailored learning experience for their learners.

## 5.6 Requirements Matching with Moodle

The purpose of this chapter is to present the mapping of the previously formulated requirements with Moodle, with the aim of ensuring that the platform meets the objectives of the CyberSecPro project, i.e. the programme's adoption and implementation by the HEIs. To mitigate any bias from existing solutions, the requirements were derived based on user stories. In total, 461 requirements were developed to adequately address the needs of the project. Comparing each available solution with the 461 requirements would have been an arduous task. To facilitate the selection process, high-level selection criteria were established in an independent step. Thirteen commercial and open source solutions were then analysed against these high-level criteria (section 5.4). After careful analysis, it was determined that Moodle emerged as the best option for the CyberSecPro education and training programme (section 5.4.3).

To ensure that Moodle is tailored to meet the specific needs of the CSP project, this chapter undertakes the task of mapping Moodle against the previously identified requirements. This mapping exercise not only highlights the areas where Moodle already meets the requirements but also identifies areas where modifications or adaptations are necessary.

The analysis of requirements and their mapping to Moodle was conducted in a systematic manner. Each requirement was individually examined by referring to its specific attributes and expected functionalities. The Moodle platform was assessed against each requirement, evaluating its capability to adequately address and fulfil the requirement. A three-level scale was employed to categorize each requirement:

> **Native**: The requirement is natively supported by Moodle and only a proper configuration is needed to achieve the desired functionality.
>
> **Needs adaptation**: The requirement can be accommodated by Moodle; however, some modifications or adaptations are required to align Moodle with the specific requirement.
>
> **Not supported**: The requirement is not supported by Moodle without breaking compatibility.

The resulting Excel file can be found in Annex C. Out of the initial 461 requirements, Moodle was found to provide native support for 264 of them. This signifies that Moodle's existing features and capabilities align with these requirements, without requiring any additional modifications or adaptations (e.g. to the code).

For 196 requirements Moodle does provide support, however, some form of adaptation or customisation is necessary to fully meet the requirement. These requirements can still be implemented in Moodle; however, additional effort is required to align Moodle with the specific needs. For instance, the institution concept is not implemented in Moodle, but is available in Moodle Workplace. Therefore, Moodle can implement the institution concept, but modifications in the database and the creation of additional forms is required.

Only one requirement out of the 461 was identified as not supported by Moodle. This particular requirement pertains to network performance and/or server versions, which are external factors that fall outside the purview of Moodle's functionalities.

Table 18 offers a comprehensive summary of the four categories of requirements, namely functional, non-functional, constraints, and supplemental. It highlights the number of requirements within each category that are natively supported, need adaptation, or are not supported at all.

Table 19: Overview of Moodle mapping against requirements sorted by category

| | Native | Needs adaptation | Not supported | Total |
|---|---|---|---|---|
| **Functional** | 201 (60%) | 136 (40%) | - | 337 |
| **Non-Functional** | 32 (48%) | 34 (51%) | 1 (1%) | 67 |
| **Constraints** | 31 (55%) | 25 (45%) | - | 56 |
| **Supplemental** | - | 1 (100%) | - | 1 |
| **Total** | 264 (57%) | 196 (43%) | 1 (0,2%) | 461 |

The main challenge in configuring Moodle to meet the DCM objectives of the CyberSecPro project will be the required dynamicity to adapt to the constantly changing cybersecurity market and curricula needs. Additionally, some specific requirements may present challenges in modifying the code without compromising compatibility. Ultimately, achieving a uniform level of functionality and efficiency across all HEIs necessitates identical Moodle site configurations. However, it is crucial to acknowledge that Moodle's functionality and effectiveness are not solely reliant on itself, but are influenced by various external factors such as network performance and server versions/updates.

Mapping the requirements to Moodle has yielded valuable insights regarding the platform's compatibility with the formulated requirements. The results indicate that the majority of the requirements have already been successfully implemented within Moodle. Considering that only one requirement is not supported, Moodle is well-equipped to meet the needs of the DCM system for the CyberSecPro education and training programme. However, it should be recognised that some requirements may require re-evaluation as the project progresses, as the necessary adaptations might fall outside the project's scope. Additionally, since the project is following an agile approach, the implementation phase will provide the opportunity to further refine, adapt, and supplement the requirements based on emerging system insights, technical challenges, and stakeholder feedback.

Nevertheless, this mapping serves as a critical step in the customisation and implementation process of the platform and will serve as foundation for the development of the DCM system in WP3. By identifying areas of alignment, necessary modifications, and potential re-evaluations, the mapping contributes to the development of a tailored system that effectively meets the specific needs of the CyberSecPro project implementation. In summary, the mapping confirms Moodle's suitability as the DCM system in the context of the CyberSecPro education and training programme. T3.2 will delve into the specific adaptation and customisation required for the "Needs adaptation" requirements, ensuring a comprehensive understanding of the implementation process.

## 5.7 Summary and Discussion

The development of 68 user stories and 461 requirements for the implementation of the dynamic curriculum management (DCM) system is a noteworthy achievement in the progress of the project. The careful categorisation of these requirements into functional, non-functional, constraint, and supplemental categories provides a comprehensive understanding of the system's needs. Furthermore, the classification of each requirement according to its priority is an important achievement, allowing the focus on the most crucial aspects during development and implementation. However, it is important to acknowledge that these requirements should be considered as preliminary. Adopting an agile approach means that new insights about the system will emerge, technical challenges will arise, and stakeholder

inputs will be received during the implementation phase. These factors may necessitate refining, adapting, and supplementing the initial set of requirements. While the prioritisation of requirements helps streamline the process and focus resources, it must be recognised that flexibility and adaptability are critical in order to meet the evolving needs of stakeholders effectively.

This chapter highlights the establishment of assessment criteria for selecting a DCM system, resulting in the identification of Moodle as the most suitable option. The mapping process that aligns the requirements of the CyberSecPro education and training program with the capabilities of Moodle shows that the chosen system already satisfies many of the identified needs. This alignment is advantageous as it ensures that the selected DCM system is equipped with features and functionalities that align with the specific requirements of the program. However, the mapping exercise also reveals areas where the Moodle system may require modifications or adaptations to fully meet the specific needs of the program.

By consistently re-evaluating requirements, the project has a better chance of meeting stakeholder needs and ultimately ensuring that the final result effectively supports and enhances the CyberSecPro education and training programme.

# 6 Concluding Remarks

The growing presence and complexity of cyber threats have made it imperative to establish strong cybersecurity training programmes. In response to this, the present deliverable endeavours to fulfil this requirement by creating the overall framework for the CyberSecPro education and training programme. Furthermore, it provides an in-depth analysis encompassing the various needs and prerequisites for its successful adoption.

This deliverable serves as a crucial starting point for the development and execution of the CyberSecPro education and training programme. It lays down a solid foundation by presenting comprehensive findings derived from extensive research and study. The analysis conducted within this document takes into account the current landscape, considering the increasing prevalence and constantly evolving nature of cyber threats.

By outlining the general structure of the CyberSecPro education and training programme, this deliverable acts as a guide for its design and implementation. It offers insights into the essential knowledge areas and training modules that need to be incorporated to ensure a comprehensive and effective training programme.

Moreover, the analysis presented in this deliverable highlights the specific needs and requirements that should be addressed while executing the CyberSecPro education and training programme. This comprehensive understanding of the needs of the different user groups ensures that the training programme is tailored to their specific requirements, maximising and effectiveness.

With the findings presented in this deliverable, the CyberSecPro education and training programme can be designed and implemented effectively. It will provide a comprehensive and relevant training experience for participants, equipping them with the necessary skills and knowledge to effectively protect European cyber infrastructure and systems.

## 6.1 CyberSecPro Knowledge Areas and training Modules

In order to create a comprehensive and effective cybersecurity education and training programme, several factors were taken into consideration in the selection of knowledge areas. These factors included market demand, relevance to the European Cybersecurity Skills Framework (ECSF), availability of education and training resources, and the importance to the protection of European cyber infrastructure and systems. By carefully analysing these factors, ten knowledge areas were identified that will shape the scope of the programme.

The identification of these knowledge areas ensures that the programme aligns with the current needs of the market and addresses relevant cybersecurity skills required in Europe. To ensure the programme's effectiveness, the existing education and training offerings by CyberSecPro partners were mapped to the identified knowledge areas. This mapping process leverages the resources and expertise already available within the partners' offerings, avoiding duplication of efforts and promoting a synergistic approach to cybersecurity education and training. Furthermore, this approach encourages collaboration and knowledge sharing among partners. This collaborative environment fosters innovation, best practices sharing, and continuous improvement in the delivery of cybersecurity education and training that is necessary in the ever-evolving landscape of cybersecurity.

## 6.2 Constraints and Requirements for the Adoption of the CyberSecPro Programme

The analysis conducted on the constraints and requirements for adopting the CyberSecPro education and training programme has provided valuable insights into the potential barriers that could hinder its adoption. These barriers encompass various aspects, including technical, business, societal, legal, and educational challenges. By identifying these barriers, the consortium gains valuable knowledge and can proactively develop strategies to mitigate potential challenges. This proactive approach enables the

consortium to be better equipped to anticipate and address any issues that may arise during the execution of the CyberSecPro programme.

However, it is essential to acknowledge that some barriers may be beyond the control of the consortium. Factors such as geopolitical situations, regulatory changes, or unforeseen events may influence the successful adoption of the programme. Additionally, some barriers may excessively burden the development or require external support to overcome. Therefore, the consortium must prioritise and focus on resolving barriers that lie within their control or influence.

## 6.3 CyberSecPro DCM system

The development of 68 user stories and 461 requirements for the implementation of the dynamic curriculum management (DCM) system marks a significant accomplishment in the project's progress. These requirements have been carefully categorised into functional, non-functional, constraint, and supplemental requirements, allowing for a comprehensive understanding of the system's needs. Furthermore, each requirement has been classified according to its priority, ensuring a clear understanding of what aspects of the system should be given higher attention during development and implementation. This prioritisation will help streamline the process and focus resources on the most crucial areas.

However, it is important to acknowledge that these requirements can only serve as a preliminary guide. Following an agile approach, it needs to be recognised that as the implementation phase progresses, new insights about the system will emerge, technical challenges will arise, and stakeholder inputs will be received. These factors may necessitate refining, adapting, and supplementing the initial set of requirements. Still, by embracing the potential for evolving requirements, the DCM system has a better chance of meeting the evolving needs of the stakeholders and supporting the project's objectives effectively. The implementation phase will provide ample opportunities to incorporate these evolving requirements, ensuring that the final result is tailored to the specific needs of the stakeholders.

Furthermore, the establishment of assessment criteria for the selection of a DCM system has provided a framework for evaluating the various systems available in the market. Through a thorough and careful evaluation process, the Moodle system has been identified as the most suitable option. The process of mapping the requirements of the CyberSecPro education and training programme to the capabilities of Moodle has shown that the system already satisfies many of the identified needs. This means that the chosen system is already equipped with features and functionalities that align with the specific requirements of the programme. However, the mapping exercise has also revealed areas where the Moodle system may require modifications or adaptations to fully meet the specific needs of the programme. Ultimately, the mapping process ensures that the selected DCM system will effectively support and enhance the CyberSecPro education and training programme.

# 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," 2023. [Online]. Available: https://www.cybersecpro-project.eu/wp-content/uploads/2023/07/D2.1_Cybersecurity_Practical_Skills_Gaps_in_Europe_v.1.0.pdf.

[2] CyberSecPro Consortium, "Blended CyberSecPro technological training interactive technologies and academic practice," *(unpublished),* 2023.

[3] "CyBOK – The Cyber Security Body of Knowledge," [Online]. Available: https://www.cybok.org/. [Accessed 06 April 2023].

[4] "National Institute for Standards and Technology - NICE Framework.," [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice. [Accessed 19 07 2023].

[5] "ENISA Cybersecurity Market Analysis Framework (ECSMAF) -V2.0"," European Union Agency for Cybersecurity , [Online]. Available: https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0. [Accessed 19 07 2023].

[6] ENISA, "European Cybersecurity Skills Framework (ECSF)," September 2022.

[7] E. Karanja and M. A. Rosso, "The Chief Information Security Officer: An Exploratory Study," *Journal of International Technology and Information Management,* vol. 26, no. 2, 2017.

[8] A. Simister, "Are CISOs in High Demand?," [Online]. Available: https://www.lepide.com/blog/are-cisos-in-high-demand/ [LL1] .

[9] ISO/IEC, "ISO/IEC 27001 Standard – Information Security Management Systems," 2022. [Online]. Available: https://www.iso.org/standard/27001. [Accessed 03 September 2023].

[10] NICCS, "Workforce Framework for Cybersecurity (NICE Framework)," NICCS, [Online]. Available: https://niccs.cisa.gov/workforce-development/nice-framework. [Accessed 15 August 2023].

[11] CIS, "Centre for Internet Security," CIS, 2023. [Online]. Available: https://www.cisecurity.org. [Accessed 03 September 2023].

[12] A. Rashid, A. Martin, S. Schneider and Y. Cherdantseva, "The Cyber Security Body Of Knowledge," [Online]. Available: https://www.cybok.org/. [Accessed 19 07 2023].

[13] Department of Homeland Security, National Institute of Standards & Technology, "National Institute of Standards & Technology," [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice. [Accessed 19 07 2023].

[14] Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques, "ISO (the International Organization for Standardization)," [Online]. Available: https://www.iso.org/standard/72437.html. [Accessed 19 July 2023].

[15] D. Wright, N. Tomić, S. Portesi and L. Marinos, "European Union Agency for Cybersecurity," 27 March 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0. [Accessed 19 07 2023].

[16] S. Samonas and D. Coss, "THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY," *Journal of Information System Security,* vol. 10, no. 3.

[17] A. C. Brualdi Timmins, "Multiple intelligences: Gardner's theory," *Practical Assessment, Research, and Evaluation,* 5(1), 10 1996.

[18] A. App, "Gardner's Theory of Multiple Intelligences, Methodologies," July 2021. [Online]. Available: https://additioapp.com/en/gardners-theory-of-multiple-intelligences/.

[19] I. Falciani, ""Flipped classroom"," *Europass Teacher Academy,* 2020.

[20] P. Dawson and L. Abeysekera, "Motivation and cognitive load in the flipped classroom: definition, rationale and a call for research," *Higher Education Research & Development,* no. 34 (1): 1–14, 2015.

[21] The Derek Bok Center for Teaching and Learning, " Flipped Classroom," Harvard University, [Online]. Available: https://bokcenter.harvard.edu/flipped-classrooms. [Accessed 03 06 2023].

[22] L. Florian and K. Black-Hawkins, "Exploring inclusive pedagogy," *British Educational Research Journal,* no. 37:5, pp. 813-828, DOI: 10.1080/01411926.2010.501096, 2011.

[23] D. Cobley, Disability and international development: A guide for learners and practitioners, London: Routledge, 2018.

[24] L. Florian, K. Black-Hawkins and M. Rouse, Achievement and inclusion in schools (2nd ed.), London: Routledge, 2017.

[25] M. Ainscow, T. Booth and A. & Dyson, Improving Schools, Developing Inclusion (1st ed.), Routledge, 2006.

[26] A. Molina, "Inclusive education in higher education: challenges and opportunities," *European Journal of Special Needs Education,* no. 32, 1, pp. 3-17, 2017.

[27] . Cook and . Rao, "Systematically applying UDL to effective practices for learners with learning disabilities," *Learning disability quarterly,* no. 41, p. 179–191, 2018.

[28] S. L. Craig, S. J. Smith and B. B. Frey, "Professional development with universal design for learning: supporting teachers as learners to increase the implementation of UDL," *Professional Development in Education,* no. 48:1, pp. 22-37, 2022.

[29] S. Valiandes, "Evaluating the impact of differentiated instruction on literacy and reading in mixed ability classrooms: Quality and equity dimensions of education effectiveness," *Studies in Educational Evaluation,* no. 15, pp. 17-26, 2015.

[30] A. A. Gokhale, "Collaborative learning enhances critical thinking," *J. Educ.,* no. 7, p. 22–30, 1995.

[31] L. Vygotsky, Mind in Society: The Development of Higher Psychological Processes, Cambridge: Harvard University Press, 1978.

[32] L. Lin, Exploring Collaborative Learning: Theoretical and Conceptual Perspectives. Investigating Chinese HE EFL Classroom, Berlin: Springer-Verlag, 2015.

[33] C. Alcaraz, R. Roman, E. Abdo-Sánchez, R. Halir, A. Hernádez-Escobar and J. Toutouh, "Gamification Models and Tools According to Profiles: An Experience in Engineering Degrees," *ICERI2019, IATED,* pp. 7740-7747, 2019.

[34] C. Wang and L. Huang, "A Systematic Review of Serious Games for Collaborative Learning: Theoretical Framework, Game Mechanic and Efficiency Assessment.," *International Journal of Mechanical Engineering Education,* vol. 16, no. 6, 2021.

[35] A. P. Markopoulos, A. Fragkou, P. D. Kasidiaris and J. P. Davim, "Gamification in engineering education and professional training," *International Journal of Mechanical Engineering Education,* vol. 43, no. 2, pp. 118-131, 2015.

[36] C. Alcaraz, E. Abdo-Sánchez, J. Toutouh, R. Halir, M. Ruiz and D. H. Stolfi, "Some ingredients to improve gamification in engineering," *EDULEARN18 Proceedings IATED,* pp. 7040-7044, 2018.

[37] S. K. Thiel, M. Reisinger, K. Röderer and M. Baldauf, "Inclusive Gamified Participation: Who are we inviting and who becomes engaged?," *52nd Hawaii International Conference on System Sciences 2019 (HICCS,* pp. 3151-3160, 2019.

[38] A. R. Dantas, M. de Oliveira Barros and C. M. L. Werner, "A Simulation-Based Game for Project Management Experiential Learning," *SEKE,* vol. 19, no. 24, June 2004.

[39] G. Gay, "Culturally responsive teaching: Theory, research, and practice (2nd ed.," *NY: Teachers College Press,* 2010.

[40] B. Sohrabi and H. Iraj, "Implementing flipped classroom using digital media: A comparison of two demographically different groups perceptions," *Computers in Human Behavior,* no. 60, pp. 514-524, 2016.

[41] L. M. Blaschke, " Heutagogy and lifelong learning: A review of heutagogical practice and self-determined learning," *The International Review of Research in Open and Distributed Learning,* vol. 13, no. 1, pp. 56-71, 2012.

[42] M. D. Ginsburg-Block, C. A. Rohrbeck and J. W. Fantuzzo, "A meta-analytic review of social, self-concept, and behavioral outcomes of peer-assisted learning," *Journal of Educational Psychology,* vol. 98, no. 4, pp. 732-749, 2006.

[43] J. J. Serrano-Aguilera, A. Tocino, S. Fortes, C. Martín, P. Mercadé-Melé, R. Moreno-Sáez and A. Torres, "Using peer review for learner performance enhancement: Experiences in a multidisciplinary higher education setting," *Education Sciences,* vol. 11, no. 2, p. 71, 2021.

[44] A. Toulia, V. Strogilos and A. E., "Peer tutoring as a means to inclusion: a collaborative action research projec," *Educational Action Research,* vol. 31, no. 2, pp. 213-229, 2023.

[45] C. Martín, A. Muñoz, A. Tocino, R. Moreno-Sáez and S. Fortes, "An Application of Peer Review and Project-Based Learning with the Aim of Boost Learners' Employability".

[46] T. Reeves, Interactive Learning, Encyclopedia of the Sciences of Learning, N. M. Seel, Ed., Boston, MA: Springer, 2012, pp. 1602-1604.

[47] T. Reeves, Interactive Learning Techniques, Encyclopedia of the Sciences of Learning, N. (. Seel, Ed., Boston, MA: Springer, 2012, pp. 1601-1611.

[48] C. Farley, "NYU Steinhardt," The Research Alliance for New York City Schools, 05 2020. [Online]. Available: https://steinhardt.nyu.edu/sites/default/files/2021-03/Research_Alliance_Summary_of_Evidence_on_Remote_and_Blended_Learning_November_2020.pdf. [Accessed 03 06 2023].

[49] A. Konstantinidis, P. M. Papadopoulos, T. Tsiatsos and S. Demetriadis, "Selecting and Evaluating a Learning Management System: A Moodle Evaluation Based on Instructors and Students.," *International Journal of Distance Education Technologies (IJDET),* vol. 9, no. 3, pp. 13-30, 2011.

[50] C. Wright, V. Lopes, T. Montgomerie, S. Reju and S. Schmoller, "Selecting a Learning Management System: Advice from an Academic Perspective," 2014.

[51] K. L. Smart and J. J. Cappel, "Students' perceptions of online learning: A comparative study," *Journal of Information Technology Education,* vol. 5, pp. 201-219, 2006.

[52] A. Sangrà, D. Vlachopoulos and N. Cabrera, "Building an Inclusive Definition of e-Learning: An Approach to the Conceptual Framework.," *The International Review of Research in Open and Distributed Learning,* vol. 13, no. 2, pp. 145-159, 2012.

[53] T. Bates, "Teaching in a Digital Age: Guidelines for Designing Teaching and Learning. 2nd Edition. Chapter 9: Choosing and Using Media in Education: The SECTIONS Model.," 2109. [Online]. Available: https://pressbooks.bccampus.ca/teachinginadigitalagev2/.

[54] "Moodle (n.d.)," [Online]. Available: https://moodle.org.

[55] R. Kay, "Exploring the Use of Video Podcasts in Education: A Comprehensive Review of the Literature," *Computers in Human Behavior,* vol. 28, no. 3, pp. 820-831, 2012.

[56] T. C. Reeves and P. M. Reeves, "Effective Dimensions of Interactive Learning on the Wolrd Wide Web. In B. Khan (Ed.)," *Web-Based Instruction, Educational Technology Publications,* pp. 59-66, 1997.

[57] P. Long and G. Siemens, "Penetrating the Fog: Analytics in Learning and Education," *EDUCAUSE Review,* vol. 46, no. 5, pp. 30-32, 2011.

[58] M. Boekaerts and L. Corno, "Self-Regulation in the Classroom: A Perspective on Assessment and Intervention.," *Applied Psychology: An International Review,,* vol. 54, no. 2, pp. 199-231, 2005.

[59] D. Mioduser, R. Nachmias, O. Lahav and A. Oren, "Web-Based Learning Environments; Current pedagogical and technological state," *Journal of Research on Computing in Education,* vol. 33, no. 1, pp. 55-76, 2000.

[60] J. Dron and T. Anderson, "Teaching crowds: Learning and social media," *Athabasca University Press,* 2014.

[61] M. Dougiamas and P. C. Taylor, "Moodle: Using learning communities to create an open source course management system," *In World Conference on Educational Multimedia, Hypermedia and Telecommunications,* vol. 2003, no. 1, pp. 171-178, 2003.

[62] M. Machado and E. Tao, "Blackboard vs. moodle: Comparing user experience of learning management systems," *2007 37th Annual Frontiers In Education Conference - Global Engineering: Knowledge Without Borders, Opportunities Without Passports, Milwaukee, WI, USA, 2007,* pp. pp. S4J-7-S4J-12, 2007.

[63] H. Coates, R. James and G. Baldwin, "A critical examination of the effects of learning management systems on university teaching and learning.," *Tertiary Education and Management,* vol. 11, no. 1, pp. 19-36, 2005.

[64] [Online]. Available: https://moodle.org/plugins/.

[65] N. Krejic, "Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analyses," 3 August 2023. [Online]. Available: https://ecmiindmath.org/2023/08/03/cybersecurity-practical-skills-gaps-in-europe-market-demand-and-analyses/.

[66] N. Krejic, "European Consortium for Mathematics in Industry," 3 August 2023. [Online]. Available: https://ecmiindmath.org/2023/08/03/cybersecurity-practical-skills-gaps-in-europe-market-demand-and-analyses/.

[67] "ISO (International Organization for Standardization)," [Online]. Available: https://www.iso.org/standard/27001. [Accessed 03 September 2023].

[68] "NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES," Office of the Chief Learning Officer (OCLO), Cybersecurity and Infrastructure Security Agency (CISA), [Online]. Available: https://niccs.cisa.gov/workforce-development/nice-framework. [Accessed 15 August 2023].

[69] "Center for Internet Security," [Online]. Available: https://www.cisecurity.org . [Accessed 03 September 2023].

[70] T. D. B. C. f. T. a. Learning, "Flipped Classroom," Harvard University, [Online]. Available: https://bokcenter.harvard.edu/flipped-classrooms. [Accessed 3 June 2023].

References

# Annex A: Template for User Stories

# USE CASE TEMPLATE

# [TITLE] USE CASE

### Document Information

| | |
|---|---|
| **Document Title** | *Title of use case – Verb Noun phrasing is almost always the most appropriate!* |
| **Document Owner** | |
| **Version** | |
| **Status** | |
| **Date** | |

## 1. BRIEF DESCRIPTION

*Insert a 1-2 sentence description of this use case. Be sure to include a starts when / ends when statement to clarify the beginning and ending points of the scope of this process or piece of functionality.*

## 2. ACTORS

*List any roles or systems involved with this process or use case. A person or system fulfilling a role will be the actor in one of the steps.*

- 

## 3. PRE-CONDITIONS

*List anything that must be true before this process or functionality begins. Preconditions should be states that a system can validate to be true. A common example is that a specific Actor has logged into the System.*

-

## 4. Basic Flow

*The basic flow is the normal course of events, otherwise called the "happy path." Ask yourself, what happens most of the time and you'll discover the steps that belong here. You'll want your basic flow to cover the full scope of activities between the starts when and ends when.*

*Create a numbered list of each step below. I recommend using the Word "numbered list" functionality to automatically number the list.*

1.

## 5. Alternate/Exception Flows

*An alternate flow is a variation from the basic flow. Alternatives can be triggered at any step in the basic flow and often reinsert the actors back into the basic flow.*

*An exception flow is an error, or a negative condition. When an exception is encountered, it prevents the process from finishing through to its conclusion until it's addressed.*

*Number your alternate and exception flows to indicate the step at which the variation occurs. For example, a variation on step 3 could be listed as 3a and a second variation as 3b, and so forth.*

*Describe the alternate functionality and then identify at what step in the basic flow this variation picks back up. For exception flows that result in the use case ending, simply write, "Use Case Ends."*

1a -

## 6. Post Conditions

*Post-conditions indicate what must be true of the state of the system after the steps of the use case are complete. These should be true for the basic flow and all alternate flows. Exception flows may have different post-conditions or none at all.*

-

## 7. Supplemental Requirements

*This is a special section I use to hold miscellaneous requirements related to the use case. Often you'll find BAs including a Business Rules section or other collection of information related to the use case. These may or may not be actual requirements – you'll want to establish a clear pattern and communicate that*

*clearly and ensure it's consistent with how your organization documents this type of requirement. I've also used this section to capture the most salient decisions and notes so they are stored right with the use case for future consideration.*

# 8. Visual Model

*Many use cases are enhanced by a visual model. A simple work-flow diagram can be used to visually show the sequence of steps and alternate and exception flows. A user interface mock-up can be used to show a possible representation of these user requirements in an interface (or a desired representation). In some organizations, a more formal UML diagram may be appropriate.*

## Revision History

| V. | Date | Author | Description | Status |
|---|---|---|---|---|
| | | | | |
| | | | | |

# Annex B: Matching of Requirements for DCM System with Moodle

| User Story | Moodle Supported | Comments | Classification | Priority | Name | Short Description | Rationale |
|---|---|---|---|---|---|---|---|
| 000_ALL | *Native* | | Non-Functional | Should have | Error Handling | Proper error messages should be displayed in different scenarios like validation errors, no internet connection, server issues or others and administrators should be notified if any issues occur while creating notifications. | To promptly inform about issues. |
| 000_ALL | *Native* | | Non-Functional | Should have | User-Friendly Interface | The platform should have an intuitive and clear interface for smooth user navigation. | To enhance user experience and efficiency during account creation. |
| 000_ALL | *Not supported* | Not related to moodle but the server network performance and versions | Non-Functional | Should have | Efficiency | The platform should be quick and efficient, quickly retrieving, validating, updating and displaying data. The user should feel instant reaction from the platform. | To ensure a smooth and efficient user experience. |
| 000_ALL | *Native* | | Constraints | Must have | Server Availability | The server should be up and running. | To ensure that the platform is accessible. |
| 000_ALL | *Native* | | Constraints | Must have | Internet Connection | An active internet connection is required. | To ensure that the user can access the platform and submit the form. |
| 000_ALL | *Native* | | Constraints | Must have | Database Availability | The databases should be available and updated. | To ensure the availability of necessary data for adding new users. |
| 101-Create Account | *Native* | | Functional | Must have | Editable Fields for Account Information | The platform should display a form with editable fields (username, password, email, etc.) for account creation. | To collect necessary information for creating a user account. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 101-Create Account | *Native* | | Functional | Must have | Access to Create Account Option | The platform must provide a visible and accessible "Create Account" button for Users. | To enable users to initiate the account creation process. |
| 101-Create Account | *Native* | | Constraints | Could have | Email Verification | Account activation should be done through email verification for security purposes. | To ensure account security and verify the authenticity of the user. |
| 101-Create Account | *Native* | | Functional | Must have | Account Verification | The platform should send an email for account verification and activate the account once the verification link is clicked. | To ensure the authenticity and verification of the user account. |
| 101-Create Account | *Native* | | Functional | Must have | Account Creation | The platform must create the user account upon submission of filled required fields. | To finalize the account creation process. |
| 101-Create Account | *Native* | | Non-Functional | Should have | Prompt and Clear Notifications | The platform must provide clear and timely notifications for errors or issues during account creation. | To keep the user informed and ensure smooth account creation process. |
| 101-Create Account | *Native* | | Non-Functional | Should have | Secure Data Handling | The platform should ensure the security and confidentiality of user data during account creation and verification. | To protect user data and ensure privacy and security. |
| 102-Edit Account | *Native* | | Functional | Must have | Editable Fields for Account Information | The platform should display a form with editable fields (username, password, email, etc.) for account creation. | To collect necessary information for editing a user account. |
| 102-Edit Account | *Native* | | Functional | Must have | Access to Edit Account Option | The platform must provide a visible and accessible "Edit Account" option for Users. | To enable users to initiate the account editing process. |
| 102-Edit Account | *Native* | | Functional | Must have | Update Confirmation | The platform should provide a confirmation message upon successful account update. | To ensure the user is informed of the successful update. |
| 102-Edit Account | *Native* | | Functional | Must have | Account Update | The platform must update the user account upon submission of edited fields. | To finalize the account editing process. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 102-Edit Account | *Native* | | Non-Functional | Should have | Prompt and Clear Notifications | The platform must provide clear and timely notifications for errors or issues during account editing. | To keep the user informed and ensure smooth account editing process. |
| 102-Edit Account | *Native* | | Non-Functional | Should have | Secure Data Handling | The platform should ensure the security and confidentiality of user data during account editing and updating. | To protect user data and ensure privacy and security. |
| 103-Delete Account | *Native* | Privacy settings: Contact the privacy officer = ENABLED | Functional | Must have | Account Deletion | The platform should delete the account after the specified period if not cancelled by the user. | To complete the account deletion process. |
| 103-Delete Account | *Native* | | Functional | Must have | Access to Delete Account Option | The platform must provide a visible and accessible "Delete Account" option for Users. | To enable users to initiate the account deletion process. |
| 103-Delete Account | *Needs adaptation* | The user must be logged in the DCM | Functional | Must have | Confirmation for Account Deletion | The platform should display a confirmation box and ask for the account password to confirm the deletion. | To ensure that the user genuinely wants to delete the account and prevent accidental deletions. |
| 103-Delete Account | *Native* | Privacy and policies: Contact the privacy officer | Functional | Must have | Account Deletion Process | The platform must mark the account as "Pending Deletion" and inform the user about the process. | To inform the user about the deletion process and offer a chance to cancel the deletion request. |
| 103-Delete Account | *Needs adaptation* | | Non-Functional | Should have | Clear and Timely Notifications | The platform must provide clear and timely notifications and information regarding account deletion. | To keep the user informed and ensure smooth account deletion process. |
| 103-Delete Account | *Native* | | Non-Functional | Should have | Secure Data Handling | The platform should ensure the security and confidentiality of user data during the account deletion process. | To protect user data and ensure privacy and security. |
| 104-Login | *Native* | | Functional | Must have | Password Recovery Option | The platform must provide an option for password recovery. | To assist users who have forgotten their passwords. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 104-Login | *Native* | | Functional | Must have | Login Option Accessibility | The platform must have a visible and accessible "Login" option. | To enable users to initiate the login process. |
| 104-Login | *Native* | | Functional | Must have | Credential Verification | The platform must verify the user credentials for login. | To ensure that only authorized users can log in. |
| 104-Login | *Native* | | Functional | Must have | Password Reset Process | The platform should facilitate the password reset process via email. | To ensure users can successfully reset their passwords and regain account access. |
| 104-Login | *Native* | | Functional | Must have | Error Notification | The platform should notify the user if the entered credentials are invalid. | To inform the user about incorrect credentials and prevent unauthorized access. |
| 104-Login | *Native* | | Non-Functional | Should have | Timely Notifications | Clear and timely notifications regarding login errors and password recovery must be provided. | To keep the user informed and ensure smooth login and password recovery processes. |
| 104-Login | *Native* | | Non-Functional | Should have | Secure Authentication Process | The platform must ensure the secure handling of user credentials during login. | To protect user credentials and ensure privacy and security. |
| 105-Link User Accounts | *Native* | Linked logins | Non-Functional | Should have | Security | Ensure the secure linking of multiple accounts, protecting user information and credentials. | To protect user data and credentials during the account linking process. |
| 105-Link User Accounts | *Native* | | Functional | Must have | Credential Verification for Linking | The platform must verify the credentials for the account to be linked. | To ensure that the user has authorization to link the accounts. |
| 105-Link User Accounts | *Native* | | Functional | Must have | Linking Option | The platform must provide an option for linking multiple accounts. | To facilitate the linking of multiple accounts for unified access. |
| 105-Link User Accounts | *Native* | | Functional | Must have | Error Notification | Notify the user in case of errors such as invalid credentials or connection issues. | To keep the user informed and ensure smooth account linking process. |
| 105-Link User Accounts | *Native* | | Functional | Must have | Unified Access | The platform must allow unified access to contents from all linked accounts. | To provide seamless access to all account contents post linking. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 106-Edit Preferences | *Native* | | Non-Functional | Should have | Security | Ensure secure editing of preferences, especially personal and privacy-related information. | To safeguard users' personal and privacy-related information. |
| 106-Edit Preferences | *Native* | | Functional | Must have | Preferences Option | The platform must provide an option for users to edit preferences. | To allow users to customize their account settings and preferences. |
| 106-Edit Preferences | *Needs adaptation* | | Functional | Must have | Email Validation for Personal Info Change | Send a validation email if email or password is edited. | To ensure the authenticity and security of personal information changes. |
| 106-Edit Preferences | *Native* | | Functional | Must have | Information Saving | The platform must save the new preferences information. | To ensure users' new preferences are applied to their account. |
| 106-Edit Preferences | *Native* | | Functional | Must have | Form Presentation | Display forms with available data and defaults for selected preferences. | To guide users in editing their preferences effectively. |
| 106-Edit Preferences | *Native* | | Functional | Must have | Display Update | Update the display based on changes in preferences. | To immediately reflect the changes made in preferences for the user. |
| 107-Search Users | *Native* | | Functional | Must have | Permission Validation | The platform must validate the user's permission to perform the search. | To ensure only authorized users can search for other users, ensuring privacy and security. |
| 107-Search Users | *Needs adaptation* | Global search | Functional | Must have | Search Form Presentation | Display a search form with criteria options for user search. | To allow users to specify their search criteria for finding other users. |
| 107-Search Users | *Native* | | Functional | Must have | Search Execution and Results Return | Execute the search and return the results to the user. | To ensure users receive the results of their search queries. |
| 107-Search Users | *Native* | | Functional | Must have | Search Option | The platform must provide a search option for users to search for other users. | To facilitate user search functionality on the platform. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 107-Search Users | *Needs adaptation* | Privacy rights must be ensured | Non-Functional | Should have | Privacy Protection | Ensure that user searches do not breach other users' privacy rights. | To protect the privacy of users on the platform. |
| 108-Search and Contact Institutions | *Needs adaptation* | Institutions are not native in Moodle. Options:<br>- Institutions plugin<br>- Moodle workplace<br>- Courses categories | Functional | Must have | Contact Institution Option | The platform must provide an option to contact the institutions from the search results. | To enable users to communicate with institutions. |
| 108-Search and Contact Institutions | *Needs adaptation* | | Functional | Must have | Message Delivery to Institution | The platform must deliver the user's message to the institution's inbox and notify the institutional contact. | To ensure effective communication between users and institutions. |
| 108-Search and Contact Institutions | *Needs adaptation* | | Functional | Must have | Search Option for Institutions | The platform must provide a search option for users to search for institutions. | To facilitate institution search functionality on the platform. |
| 108-Search and Contact Institutions | *Needs adaptation* | | Non-Functional | Should have | Privacy and Permission Handling | Ensure that user searches and contacts adhere to privacy standards and permission levels. | To protect privacy and ensure communication is within allowed permissions. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 111-Create Notifications | *Needs adaptation* | | Constraints | Could have | Complete Event Information | All fields required by the template should be provided by the event. | To ensure complete and accurate information in the notification message. |
| 111-Create Notifications | *Needs adaptation* | | Constraints | Could have | Template Availability | Templates should be available for each type of event triggering a notification. | To ensure consistent and standardized notification messages. |
| 111-Create Notifications | *Needs adaptation* | | Functional | Must have | Recipient List Creation | The system should generate a list of users that should receive the notification. | To ensure that the notification is sent to all relevant users. |
| 111-Create Notifications | *Needs adaptation* | | Functional | Must have | Message Template Retrieval | The system should search for the appropriate message template for the triggered event. | To ensure that the notification message is in the correct format. |
| 111-Create Notifications | *Needs adaptation* | | Functional | Must have | Email Notification Sending | The system should send the notification by email to every user on the list. | To ensure users receive notifications by email if they have selected this option. |
| 111-Create Notifications | *Needs adaptation* | | Functional | Must have | Platform Notification Sending | The system should send the notification through the internal message system to every user in the list. | To ensure users receive notifications within the platform. |
| 111-Create Notifications | *Needs adaptation* | | Functional | Must have | Notification Triggering | The system should be able to trigger a notification based on specific events. | To initiate the notification creation process based on specific events. |
| 111-Create Notifications | *Needs adaptation* | | Functional | Must have | Message Composition | The system should compose the message by replacing placeholders with the event information. | To personalize the notification message with event-specific information. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 111-Create Notifications | *Needs adaptation* | | Functional | Must have | Email List Creation | The system should generate a list of users who prefer to receive the notification via email. | To respect users' preferences regarding notification delivery method. |
| 201-Create Institution | *Needs adaptation* | | Functional | Must have | Form Filling | The Institution Manager should fill in the details of the Institution including Name, Shortname, Contacts, etc. | To provide necessary information for institution creation. |
| 201-Create Institution | *Needs adaptation* | | Functional | Must have | Add/Invite Users | The Institution Manager should be able to Add/Invite Users to the Institution. | To add members to the institution. |
| 201-Create Institution | *Needs adaptation* | | Functional | Must have | Validation of Form Fields | The platform should validate the form fields. | To ensure accurate and complete information is provided. |
| 201-Create Institution | *Needs adaptation* | | Constraints | Could have | Complete Information | All required fields in the form must be filled. | To ensure that sufficient information is provided for institution creation. |
| 201-Create Institution | *Needs adaptation* | | Functional | Must have | Institution Creation | The platform should create the Institution after successful validation. | To finalize the institution creation process. |
| 201-Create Institution | *Needs adaptation* | | Non-Functional | Should have | Prompt Error Messages | The platform should provide prompt and clear error messages. | To inform the user about errors or missing information. |
| 201-Create Institution | *Needs adaptation* | | Functional | Must have | Access to Institution Menu | The Institution Manager should be able to access the Institution menu. | To initiate the institution creation process. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 201-Create Institution | *Needs adaptation* | | Functional | Must have | Initiate Institution Creation | The Institution Manager should be able to click on the "Create Institution" button. | To proceed with the institution creation process. |
| 201-Create Institution | *Needs adaptation* | | Functional | Must have | Create Institution Profiles | The Institution Manager should have an option to create Institution profiles. | To set up profiles within the institution. |
| 201-Create Institution | *Needs adaptation* | | Functional | Must have | Submit Information | The Institution Manager should be able to submit the filled form. | To submit information for institution creation. |
| 202-Manage Institution | *Needs adaptation* | | Constraints | Could have | Complete Information | All required fields in the form must be filled. | To ensure that sufficient information is provided for institution management. |
| 202-Manage Institution | *Needs adaptation* | | Functional | Must have | Validation of Form Fields | The platform should validate the form fields. | To ensure that the provided information is correct and complete. |
| 202-Manage Institution | *Needs adaptation* | | Functional | Must have | Update Institution Details | The platform should update the Institution details after successful validation. | To finalize the institution management process. |
| 202-Manage Institution | *Needs adaptation* | | Non-Functional | Should have | Prompt Error Messages | The platform should provide prompt and clear error messages. | To inform the user about errors or missing information. |
| 202-Manage Institution | *Needs adaptation* | | Functional | Must have | Edit Institution Details | The User should be able to edit the desired Institution details. | To make necessary changes in the institution details. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 202-Manage Institution | *Needs adaptation* | | Functional | Must have | Initiate Institution Management | The User should be able to click on the "Manage Institution" button. | To proceed with the institution management process. |
| 202-Manage Institution | *Needs adaptation* | | Functional | Must have | Access to Institution List | The User should be able to access the Institution from the Institution list. | To select the institution for management. |
| 202-Manage Institution | *Needs adaptation* | | Functional | Must have | Submit Updated Information | The User should be able to click the "Submit" button after editing. | To submit the updated information for the institution. |
| 203-Delete Institution | *Needs adaptation* | | Non-Functional | Should have | Secure Deletion Process | The deletion process should be secure, requiring password confirmation. | To ensure the security and integrity of the deletion process. |
| 203-Delete Institution | *Needs adaptation* | | Functional | Must have | Validation for Members and Training Modules | The platform should validate that the Institution has no other members or Training Modules with users enrolled. | To ensure no dependencies exist before deletion. |
| 203-Delete Institution | *Needs adaptation* | | Constraints | Could have | Password Verification | The password entered for confirmation must be correct. | To ensure the authenticity of the deletion request. |
| 203-Delete Institution | *Needs adaptation* | | Functional | Must have | Password Confirmation | The Institution Manager should enter the password to confirm the deletion. | To ensure the security of the deletion process. |
| 203-Delete Institution | *Needs adaptation* | | Functional | Must have | Completion of Deletion | The platform should delete the institution after a certain period. | To finalize the deletion process. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 203-Delete Institution | *Needs adaptation* | | Functional | Must have | Notification of Deletion | The platform should send an email to the Institution contact and Institution Manager personal email informing that a request to delete the institution was submitted. | To notify the concerned parties about the deletion request. |
| 203-Delete Institution | *Needs adaptation* | | Functional | Must have | Initiate Institution Deletion | The Institution Manager should be able to click on the "Delete Institution" button. | To proceed with the institution deletion process. |
| 203-Delete Institution | *Needs adaptation* | | Functional | Must have | Cancellation of Deletion | The Institution Manager should be able to cancel the deletion request. | To provide an option to revoke the deletion request. |
| 203-Delete Institution | *Needs adaptation* | | Functional | Must have | Access to Institution List | The Institution Manager should be able to access the Institution from the Institution list. | To select the institution for deletion. |
| 204-Add or Invite Users to Institution | *Needs adaptation* | | Non-Functional | Should have | Secure Process | The process should be secure, ensuring that only authorized users can add or invite others to the institution. | To ensure the security and integrity of the user addition/invitation process. |
| 204-Add or Invite Users to Institution | *Needs adaptation* | | Functional | Must have | Adding Users to Institution | The platform should add the users to the Institution upon acceptance. | To complete the process of adding users to the institution. |
| 204-Add or Invite Users to Institution | *Needs adaptation* | | Constraints | Could have | User Permissions | User1 must have "Institution User Management" permission. | To ensure that only authorized users can add or invite others to the institution. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 204-Add or Invite Users to Institution | *Needs adaptation* | | Functional | Must have | User Selection and Confirmation | User1 should be able to select users from the search results and confirm the user list. | To finalize the list of users to be added or invited to the institution. |
| 204-Add or Invite Users to Institution | *Needs adaptation* | | Functional | Must have | User Search | User1 should be able to perform a User search. | To find and select the users to be added or invited to the institution. |
| 204-Add or Invite Users to Institution | *Needs adaptation* | | Functional | Must have | Initiate Adding/Inviting Users | User1 should be able to click on the "Add Users" or "Invite Users" button. | To initiate the process of adding or inviting users to the institution. |
| 204-Add or Invite Users to Institution | *Needs adaptation* | | Functional | Must have | Accepting Invitations | User2 should be able to see and accept the invitation. | To join the institution upon acceptance. |
| 204-Add or Invite Users to Institution | *Needs adaptation* | | Functional | Must have | Sending Invitations | The platform should send an invitation to each user on the list. | To notify the users about the invitation to join the institution. |
| 204-Add or Invite Users to Institution | *Needs adaptation* | | Functional | Must have | Access to Institution List | User1 should be able to access the Institution from the Institution list. | To select the institution for adding or inviting users. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 205-Create User Group | *Native* | User groups or cohorts | Functional | Must have | Input Group Details | The platform should allow the user to input group details: Group name, Group description and group type. | To provide details for the creation of the user group. |
| 205-Create User Group | *Native* | | Non-Functional | Should have | Secure Process | The process should be secure, ensuring that only authorized users can create a user group. | To ensure the security and integrity of the user group creation process. |
| 205-Create User Group | *Native* | | Functional | Must have | User Search and Selection | Users should be able to perform a user search and select users to be added to the group. | To add members to the user group. |
| 205-Create User Group | *Needs adaptation* | | Constraints | Could have | User Permissions | Users must have "Institution Group management" permission. | To ensure that only authorized users can create a user group. |
| 205-Create User Group | *Native* | | Functional | Must have | User Group Creation | The platform should create the user group upon submission. | To finalize the creation of the user group. |
| 205-Create User Group | *Native* | | Functional | Must have | Initiate User Group Creation | Users should be able to click on the "Create User Group" button. | To initiate the process of creating a user group. |
| 205-Create User Group | *Needs adaptation* | | Functional | Must have | Access to Institution | Users should be able to access the Institution where they have privileges to create user groups. | To select the institution for creating a user group. |
| 206-Manage User Group | *Native* | | Non-Functional | Should have | Secure Process | The process should be secure, ensuring that only group owners can manage the user group. | To ensure the security and integrity of the user group management process. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 206-Manage User Group | *Native* | | Functional | Must have | View and Edit Group Details | The platform should present the group details and allow the user to edit them, including adding or removing owners or members. | To provide details for the management of the user group. |
| 206-Manage User Group | *Native* | | Constraints | Could have | User Permissions | Users must be owners of a User Group. | To ensure that only authorized users can manage a user group. |
| 206-Manage User Group | *Native* | | Functional | Must have | User Group Update | The platform should update the User Group upon submission. | To finalize the management of the user group. |
| 206-Manage User Group | *Native* | | Functional | Must have | Initiate User Group Management | Users should be able to click on the "Manage User Group" button. | To initiate the process of managing a user group. |
| 206-Manage User Group | *Native* | | Functional | Must have | Access to User Group Details | Users should be able to access the User Group details where they have group owner privileges. | To select the user group for management. |
| 207-Delete User Group | *Native* | | Non-Functional | Should have | Secure Process | The process should be secure, ensuring that only group owners can delete the user group. | To ensure the security and integrity of the user group deletion process. |
| 207-Delete User Group | *Native* | | Functional | Must have | Execute User Group Deletion | Upon user confirmation, the platform should delete the User Group. | To finalize the deletion of the user group. |
| 207-Delete User Group | *Native* | | Constraints | Could have | User Permissions | Users must be owners of a User Group. | To ensure that only authorized users can delete a user group. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 207-Delete User Group | *Native* | | Functional | Must have | User Group Deletion Confirmation | The platform should ask for confirmation from the user for group deletion. | To ensure that the user intentionally wants to delete the user group. |
| 207-Delete User Group | *Native* | | Functional | Must have | Initiate User Group Deletion | Users should be able to click on the "Delete User Group" button. | To initiate the process of deleting a user group. |
| 207-Delete User Group | *Native* | | Functional | Must have | Access to User Group Details | Users should be able to access the User Group details where they have group owner privileges. | To select the user group for deletion. |
| 212-Create a Process | *Needs adaptation* | **Linked to institution - not native in Moodle (old plugin available)** | Non-Functional | Should have | Secure Process | The process should be secure, ensuring that only users with "Institution Management" permission can create a process. | To ensure the security and integrity of the process creation. |
| 212-Create a Process | *Needs adaptation* | | Constraints | Could have | User Permissions | Users must have "Institution Management" permission. | To ensure that only authorized users can create a process. |
| 212-Create a Process | *Needs adaptation* | | Functional | Must have | Test the Process | The platform should allow users to test the process. | To ensure that the process works as expected before activation. |
| 212-Create a Process | *Needs adaptation* | | Functional | Must have | Initiate Process Creation | Users should be able to click on the "Processes" menu entry and "Create Process". | To initiate the process of creating a process. |
| 212-Create a Process | *Needs adaptation* | | Non-Functional | Should have | Reliable Notifications | The platform should reliably send notifications related to the process. | To keep users informed about the process status and outcomes. |
| 212-Create a Process | *Needs adaptation* | | Functional | Must have | Submit and Activate the Process | The platform should allow users to submit and activate the process. | To make the process operational. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 212- Create a Process | *Needs adaptation* | | Functional | Must have | Define Process Rules and Results | The platform should allow users to define the process rules and results. | To outline the actions and outcomes of the process. |
| 212- Create a Process | *Needs adaptation* | | Functional | Must have | Define Process Preconditions | The platform should allow users to define the pre-conditions which will trigger the process rules. | To set the conditions under which the process will be triggered. |
| 212- Create a Process | *Needs adaptation* | | Functional | Must have | Access to Institution | Users should be able to access the Institution from the Institution list. | To start the process creation. |
| 301- Create a Training Module -- User Story | *Native* | | Functional | Must have | Form Filling | Provide forms for users to fill in mandatory fields, prerequisites, and other metadata. | To collect necessary information and details about the Training Module. |
| 301- Create a Training Module -- User Story | *Native* | | Functional | Must have | Training Module Creation | Allow users to create a new Training Module. | To enable trainers to define, characterize, and add content to a training module and submit it for approval. |
| 301- Create a Training Module -- User Story | *Native* | | Functional | Must have | Title Setting | Enable users to set a title for the Training Module. | To ensure that every Training Module has a unique and descriptive title. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 301-Create a Training Module -- User Story | *Native* | | Non-Functional | Should have | Error Notifications | Display error notifications for various issues during the Training Module creation process. | To inform trainers about errors and guide them to resolve the issues. |
| 301-Create a Training Module -- User Story | *Needs adaptation* | | Non-Functional | Should have | User Notifications | Send notifications to users regarding the submission and approval status of the Training Module. | To keep trainers informed about the status of the Training Module they have submitted. |
| 301-Create a Training Module -- User Story | *Native* | | Functional | Must have | Component Selection and Editing | Allow users to choose and edit components for the Training Module. | To let trainers customize and build the content and structure of the Training Module. |
| 301-Create a Training Module -- User Story | *Native* | | Functional | Must have | Content Addition | Enable users to add or upload initial content for the Training Module. | To populate the Training Module with relevant learning materials and content. |
| 302-Manage a Training Module -- User Story | *Native* | | Functional | Must have | Editing Environment Access | Provide access to the editing environment when the "Manage Training Module" button is clicked. | To allow users to make changes to the Training Module. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 302-Manage a Training Module -- User Story | *Needs adaptation* | | Functional | Must have | Training Module Management | Allow authorized users to manage a Training Module. | To enable Training Module Trainers or users within the Training Module Institution to edit the Training Module. |
| 302-Manage a Training Module -- User Story | *Needs adaptation* | | Functional | Must have | Training Module Change Submission | Enable users to submit changes to the Training Module for approval. | To ensure that changes to the Training Module are reviewed and approved by the Institution. |
| 302-Manage a Training Module -- User Story | *Needs adaptation* | | Non-Functional | Should have | User Notifications | Send notifications to users regarding the submission and approval status of the Training Module changes. | To keep users informed about the status of the changes they have submitted. |
| 303-Delete a Training Module -- User Story | *Needs adaptation* | | Functional | Must have | Training Module Deletion | Allow authorized users to delete a Training Module. | To enable users with "Institution Training Modules Manager" permission to remove a Training Module from the platform. |
| 303-Delete a Training Module -- User Story | *Needs adaptation* | | Constraints | Must have | User Permission | Only allow users with "Institution Training Modules Manager" permission to delete a Training Module. | To ensure that only authorized users can delete a Training Module. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 303-Delete a Training Module -- User Story | *Needs adaptation* | | Functional | Must have | Deletion Confirmation | Require users to enter a password to confirm the deletion of a Training Module. | To ensure that the deletion is intentional and authorized. |
| 303-Delete a Training Module -- User Story | *Needs adaptation* | | Functional | Should have | Deletion Notification | Send an email to the Training Module Trainers regarding the deletion request. | To inform the Trainers about the deletion request and provide them with an option to cancel the request. |
| 303-Delete a Training Module -- User Story | *Needs adaptation* | | Non-Functional | Should have | Deletion Delay | Delay the actual deletion of the Training Module for a specified period (e.g., 2 weeks). | To provide an opportunity for the Trainers to cancel the deletion request. |
| 304-AddTrainingMaterial | *Native* | | Functional | Must have | Material Visibility | Ensure new material is visible on the training module page. | To confirm the successful addition of training materials. |
| 304-AddTrainingMaterial | *Native* | | Functional | Must have | Material Type Selection | Provide options for the type of material to be added. | To enable the addition of various types of training materials. |
| 304-AddTrainingMaterial | *Native* | | Functional | Must have | Mandatory Field Validation | Validate that all mandatory fields are filled before adding material. | To ensure that all necessary information is provided. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 304-AddTrainingMaterial | *Native* | | Functional | Must have | Material Addition | Allow users to add training materials to a module. | To facilitate the addition of diverse training materials to a training module. |
| 304-AddTrainingMaterial | *Native* | | Functional | Should have | Error Notification | Notify users if not all mandatory fields are filled. | To guide users to provide all necessary information. |
| 305_EditTrainingMaterial | *Native* | | Functional | Must have | Delete Material | Provide an option for users to delete training materials. | To enable the removal of unnecessary or outdated training materials. |
| 305_EditTrainingMaterial | *Native* | | Functional | Must have | Metadata Modification | Allow users to modify the metadata of training materials. | To ensure the accurate and up-to-date information of training materials. |
| 305_EditTrainingMaterial | *Native* | | Functional | Must have | Edit Material | Allow users to edit training materials. | To facilitate the modification of training materials in a training module. |
| 305_EditTrainingMaterial | *Needs adaptation* | | Functional | Must have | Material Update Confirmation | Confirm the successful update of training materials. | To inform users of the successful modification of training materials. |
| 305_EditTrainingMaterial | *Needs adaptation* | | Functional | Should have | Deletion Warning | Warn users about the irreversibility of the deletion operation. | To prevent accidental deletion of training materials. |
| 311-Create a Learning Path | *Needs adaptation* | | Functional | Must have | Add Training Modules to Learning Path | Enable adding Training Modules to the Learning Path. | To build a comprehensive Learning Path with appropriate modules. |
| 311-Create a Learning Path | *Needs adaptation* | | Constraints | Must have | User Permissions | Only allow users with the necessary permissions to create a Learning Path. | To ensure only authorized users can create a Learning Path. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 311-Create a Learning Path | *Needs adaptation* | Moodle has learning plan | Functional | Must have | Submit Learning Path for Approval | Enable submitting the Learning Path for approval by the Institution. | To ensure the Learning Path meets the standards and requirements of the Institution. |
| 311-Create a Learning Path | *Needs adaptation* | | Functional | Must have | Create Learning Path Environment | Provide an environment for creating a Learning Path. | To facilitate the creation of a Learning Path by the user. |
| 311-Create a Learning Path | *Needs adaptation* | | Functional | Must have | Fill Learning Path Metadata | Enable filling out a form with metadata for the Learning Path. | To fully characterize the Learning Path for future users. |
| 311-Create a Learning Path | *Needs adaptation* | | Non-Functional | Should have | Error Notifications | Notify the user of any issues during the creation of a Learning Path. | To inform the user of any issues that occur during the creation of a Learning Path and guide them in resolving these issues. |
| 311-Create a Learning Path | *Needs adaptation* | | Functional | Must have | Sort Training Modules | Enable sorting the Training Modules within the Learning Path. | To provide a structured and logical flow for the Learning Path. |
| 311-Create a Learning Path | *Needs adaptation* | | Functional | Must have | Set Learning Path Title | Enable setting a title for the Learning Path. | To provide a unique identifier and description for the Learning Path. |
| 312-AssignTrainerToTrainingModule | *Needs adaptation* | | Functional | Must have | Display List of Trainers | Display a list of all registered trainers within the institution. | To allow the user to select trainers from a list. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 312-AssignTrainerToTrainingModule | *Native* | | Functional | Must have | Add Trainer to Training Module | Enable adding one or more trainers to a selected training module. | To assign suitable trainers to the training module. |
| 312-AssignTrainerToTrainingModule | *Needs adaptation* | | Constraints | Must have | Trainer Availability | Ensure trainers are registered within the institution. | To ensure only valid trainers are assigned. |
| 312-AssignTrainerToTrainingModule | *Native* | | Functional | Must have | Select Trainer and Define Role | Enable selection of a trainer and definition of their role. | To ensure trainers have defined roles in the training module. |
| 312-AssignTrainerToTrainingModule | *Native* | | Functional | Must have | Save Assigned Trainers | Enable saving the assigned trainers and their roles. | To finalize the assignment of trainers to the training module. |
| 313-RemoveTrainerFromTrainingModule | *Native* | | Functional | Must have | Display List of Assigned Trainers | Display a list of all trainers assigned to the training module. | To allow the user to select trainers to remove. |
| 313-RemoveTrainerFromTrainingModule | *Native* | | Functional | Must have | Select Trainer to Remove | Enable selection of a trainer to remove from the training module. | To ensure only selected trainers are removed. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 313-RemoveTrainerFromTrainingModule | *Native* | | Constraints | Must have | Trainer Assignment | Ensure trainers are assigned to the training module. | To ensure only valid trainers are removed. |
| 313-RemoveTrainerFromTrainingModule | *Native* | | Functional | Must have | Save Removal of Trainers | Enable saving the removal of trainers. | To finalize the removal of trainers from the training module. |
| 313-RemoveTrainerFromTrainingModule | *Native* | | Functional | Must have | Remove Trainer from Training Module | Enable removing one or more trainers from a selected training module. | To manage trainers for the training module effectively. |
| 316-Create Assignment | *Native* | | Functional | Must have | Add Assignment to Training Module | Enable adding assignments to a training module. | To allow trainers to assess trainees. |
| 316-Create Assignment | *Native* | | Functional | Must have | Form to Add Assignment | Provide a form for users to fill out assignment details. | To collect necessary information about the assignment. |
| 316-Create Assignment | *Native* | | Functional | Must have | Insert Assignment Questions | Enable users to insert questions for the assignment. | To create detailed and comprehensive assignments. |
| 316-Create Assignment | *Native* | | Functional | Must have | Select Assignment Type | Allow users to select the type of assignment. | To ensure the assignment is created as per the requirements. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 316-Create Assignment | *Native* | | Functional | Must have | Submit Assignment | Allow users to submit the assignment. | To finalize and add the assignment to the training module. |
| 316-Create Assignment | *Native* | | Constraints | Must have | User Permissions | Ensure only authorized users can add assignments. | To maintain the integrity and security of the training module. |
| 317-Edit Assignment | *Native* | | Functional | Must have | Form for Editing Assignment | Present a form for editing assignment details. | To collect updated assignment information. |
| 317-Edit Assignment | *Native* | | Constraints | Must have | User Permissions for Editing Assignment | Allow only authorized users to edit assignments. | To ensure that only authorized personnel can make changes to assignments. |
| 317-Edit Assignment | *Needs adaptation* | | Functional | Must have | Edit Assignment Questions | Allow selection and editing of assignment questions. | To ensure that questions are relevant and up-to-date. |
| 317-Edit Assignment | *Needs adaptation* | | Functional | Must have | Edit Assignment in Training Module | Allow editing of assignments in a training module. | To ensure that trainers can modify assignments as per updated requirements. |
| 317-Edit Assignment | *Needs adaptation* | | Non-Functional | Should have | Notification of Assignment Changes | Notify users about changes in the assignment. | To keep enrolled users informed about the updates. |
| 317-Edit Assignment | *Native* | | Functional | Must have | Submit Edited Assignment | Enable submission of edited assignment. | To update the assignment in the training module. |
| 318-Browse Assignment Answers | *Native* | | Functional | Must have | Browse Assignment Answers | Enable viewing of all submitted assignment answers by trainees. | To allow trainers to review and grade assignment answers. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 318-Browse Assignment Answers | *Native* | | Functional | Must have | Filter Assignment Answers | Provide a filter option for viewing assignment answers. | To assist trainers in easily finding ungraded assignment answers. |
| 318-Browse Assignment Answers | *Native* | | Constraints | Must have | Trainer Authentication | Allow only authenticated trainers to browse assignment answers. | To ensure the security and privacy of assignment answers. |
| 318-Browse Assignment Answers | *Native* | | Functional | Must have | Navigate to Assignment | Allow trainers to navigate and select a specific assignment. | To facilitate the process of browsing assignment answers. |
| 318-Browse Assignment Answers | *Native* | | Non-Functional | Should have | Timely Error Notifications | Provide timely error notifications for internet or server issues. | To keep the user informed about the system status and possible interruptions. |
| 319-Grade Assignment Answers | *Native* | | Functional | Must have | Grade Assignment Answers | Enable grading of each question in an assignment answer. | To allow trainers to evaluate and grade assignment answers. |
| 319-Grade Assignment Answers | *Native* | | Constraints | Must have | Trainer Authentication | Allow only authenticated trainers to grade assignment answers. | To ensure the security and privacy of assignment answers. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 319-Grade Assignment Answers | *Native* | | Functional | Must have | Navigate to Assignment Answers | Allow trainers to navigate and select a specific assignment answer. | To facilitate the process of grading assignment answers. |
| 319-Grade Assignment Answers | *Native* | | Functional | Must have | Set Final Grade | Allow setting a final grade for the assignment answer. | To finalize the grading process. |
| 319-Grade Assignment Answers | *Native* | | Functional | Must have | Insert Comments | Provide an option for inserting comments for each question. | To give trainers the ability to provide feedback. |
| 319-Grade Assignment Answers | *Native* | | Functional | Must have | Notification to Trainee | Send notification to the trainee post grading. | To inform trainees about their graded assignments. |
| 319-Grade Assignment Answers | *Native* | | Functional | Must have | Save Assignment Grade | Ensure the assignment grade is saved. | To keep a record of the grading. |
| 319-Grade Assignment Answers | *Needs adaptation* | | Non-Functional | Should have | Timely Error Notifications | Provide timely error notifications for internet or server issues. | To keep the user informed about the system status and possible interruptions. |
| 401-Find-Browse Learning | *Needs adaptation* | | Functional | Should have | Add Learning Path to Favourites | Users should have the option to add a learning path to their favourites. | To allow users to save learning paths they are interested in for easy access later. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 401-Find-Browse Learning Path | *Needs adaptation* | **Moodle has learning plan, not learning paths.** | Functional | Must have | Access Learning Paths | Users must be able to access the Learning Paths section. | To enable users to browse and search learning paths. |
| 401-Find-Browse Learning Path | *Needs adaptation* | | Functional | Must have | Search for Learning Paths | Users should be able to perform a search by setting certain properties. | To facilitate users in finding suitable learning paths. |
| 401-Find-Browse Learning Path | *Needs adaptation* | | Functional | Must have | View Learning Path Details | Users must be able to view full details of a selected learning path. | To give users complete information about a learning path. |
| 401-Find-Browse Learning Path | *Needs adaptation* | | Non-Functional | Should have | Timely Error Notifications | System should provide timely error notifications. | To keep users informed about the issues and enhance user experience. |
| 401-Find-Browse Learning Path | *Needs adaptation* | | Functional | Must have | View List of Learning Paths | Users should be able to view a list of learning paths. | To provide users with options and details of available learning paths. |
| 402-BrowseTraiiningModules | *Native* | Plugin: Advance course search | Functional | Must have | Search Criteria Selection | Users should be able to select and combine up to four search criteria to filter training modules. | To allow users to effectively narrow down and find relevant training modules. |
| 402-BrowseTraiiningModules | *Native* | | Functional | Must have | Access to Module Page | Users should be able to click on a particular module and be redirected to that module's page. | To allow users to explore and learn more about a particular training module. |
| 402-BrowseTraiiningModules | *Native* | Plugin: Advance course search | Constraints | Could have | Limited Search Criteria | Users can only combine up to four search criteria for filtering training modules. | To prevent overly complex searches and ensure efficient search performance. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 402-BrowseTrainingModules | *Native* | | Functional | Must have | Display of Available Modules | The system should display a list of available modules that satisfy the selected search criteria. | To provide users with a list of relevant training modules based on their search criteria. |
| 404-EnrolInTrainingModule | *Native* | | Constraints | Should have | Enrolment Key | If protected by an enrolment key, the trainee must enter a valid key to enrol. | To ensure authorized enrolment in protected modules. |
| 404-EnrolInTrainingModule | *Native* | | Functional | Must have | Enrol in Training Module | Trainees should be able to enrol in a selected training module. | To allow trainees to start the learning process in a selected module. |
| 404-EnrolInTrainingModule | *Native* | | Functional | Must have | Receive Welcome Email | System should send an automatic welcome email to the trainee upon enrolment. | To confirm enrolment and provide additional information if necessary. |
| 404-EnrolInTrainingModule | *Native* | | Functional | Must have | Access Training Modules List | Trainees must be able to access the list of available training modules. | To enable trainees to choose and enrol in a training module. |
| 404-EnrolInTrainingModule | *Native* | | Constraints | Must have | Training Module Availability | Training module must be available for enrolment. | To ensure that trainees can only enrol in available modules. |
| 404-EnrolInTrainingModule | *Native* | | Non-Functional | Should have | Timely Email Notification | System should send a welcome email promptly upon enrolment. | To ensure timely communication and confirmation to the trainees. |
| 404-EnrolInTrainingModule | *Native* | | Functional | Must have | View Module Information | System should display brief information about a selected module. | To provide necessary information to the trainees before enrolment. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 407-Get Training Module Certificate | *Native* | | Functional | Must have | Acknowledge Training Completion | The platform must acknowledge the completion of the training module. | To confirm the completion status and initiate the certificate generation process. |
| 407-Get Training Module Certificate | *Needs adaptation* | | Functional | Should have | Suggest Additional Training | The platform should suggest additional training modules. | To encourage continuous learning and exploration of other relevant modules. |
| 407-Get Training Module Certificate | *Native* | | Non-Functional | Should have | Reliable Certificate Generation | The platform must reliably generate and provide certificates. | To ensure the authenticity and reliability of the certificates. |
| 407-Get Training Module Certificate | *Needs adaptation* | | Functional | Must have | Provide Certificate Download Link | The platform must provide a link to download the certificate. | To facilitate easy and direct downloading of the certificate. |
| 407-Get Training Module Certificate | *Needs adaptation* | | Functional | Must have | List Certificate in User Profile | The platform must add the certificate to the user's profile. | To keep a record and easy access to the certificate for the user. |
| 407-Get Training Module Certificate | *Native* | | Functional | Must have | Generate Certificate | The platform must generate a certificate upon completion of the training module. | To provide a proof of completion to the users. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 408-Share Training Certificate | *Needs adaptation* | | Functional | Should have | Share on Social Media | The platform should facilitate sharing on social media platforms. | To enhance the reach and visibility of the certificate. |
| 408-Share Training Certificate | *Native* | | Constraints | Must have | Valid Email for Sharing | A valid email address is required for email sharing. | To ensure successful email sharing. |
| 408-Share Training Certificate | *Needs adaptation* | | Functional | Should have | Email Certificate | The platform should send the certificate to a specified email. | To facilitate direct sharing via email. |
| 408-Share Training Certificate | *Needs adaptation* | | Functional | Must have | Share Certificate Options | The platform must provide options for sharing the certificate. | To facilitate the sharing process according to user preference. |
| 408-Share Training Certificate | *Native* | | Functional | Must have | Access to Completed Training | The user must be able to access their completed training. | To initiate the process of sharing the certificate. |
| 408-Share Training Certificate | *Needs adaptation* | | Non-Functional | Should have | Secure Sharing | The platform must ensure secure and reliable sharing. | To maintain the integrity and confidentiality of the certificate. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 408-Share Training Certificate | *Needs adaptation* | | Functional | Must have | Generate Shareable Link | The platform must generate a shareable link. | To provide a means for users to share the certificate easily. |
| 408-Share Training Certificate | *Native* | | Functional | Should have | View Certificate Details | The user should be able to view their certificate details. | To verify the information before sharing. |
| 410-Get Aggregate Training Results | *Native* | | Functional | Must have | View All Training Results | Users should be able to view a summary of all their training results and certificates. | To allow users to review their overall training achievements. |
| 410-Get Aggregate Training Results | *Needs adaptation* | | Functional | Must have | Generate Shareable Link | The platform must be able to generate a shareable link. | To enable users to share their training achievements. |
| 410-Get Aggregate Training Results | *Needs adaptation* | | Functional | Must have | Access to Completed Training | Users should be able to access their completed training. | To facilitate the viewing of aggregate training results. |
| 410-Get Aggregate Training Results | *Needs adaptation* | | Functional | Must have | Naming the Shared Page | Users should be able to name the page to be shared. | To personalize the shared training achievements page. |
| 410-Get Aggregate Training Results | *Needs adaptation* | | Non-Functional | Should have | Security | Ensure the secure generation and sharing of training information. | To safeguard users' training information and certificates. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 411-Get Individual Training Module Results | *Native* | | Functional | Must have | View Basic Information and Certificate | Users should be able to view basic information and the certificate. | To allow users to review their basic training module achievements. |
| 411-Get Individual Training Module Results | *Needs adaptation* | | Non-Functional | Should have | Performance | The platform should load the training module details efficiently. | To ensure quick access to training module details. |
| 411-Get Individual Training Module Results | *Native* | | Functional | Must have | Access Individual Training Module | Users should be able to access individual completed training modules. | To facilitate the viewing of individual training module results. |
| 411-Get Individual Training Module Results | *Native* | | Functional | Must have | View Detailed Training Module Information | Users should be able to view detailed information for a selected training module. | To provide comprehensive information on training module completion. |
| 412-Browse Similar Training Modules | *Needs adaptation* | | Functional | Must have | Search Based on Module Details | The platform should be able to perform a search based on the details of the selected training module. | To ensure accurate and relevant search results. |
| 412-Browse Similar Training Modules | *Needs adaptation* | | Non-Functional | Should have | Performance | The platform should return the list of similar training modules quickly. | To ensure efficient browsing of similar training modules. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 412-Browse Similar Training Modules | *Needs adaptation* | | Functional | Must have | Access Similar Training Modules Option | Users should be able to select an option to find similar training modules. | To facilitate the browsing of similar training modules. |
| 412-Browse Similar Training Modules | *Needs adaptation* | | Functional | Must have | Display List of Matching Modules | The platform should display a list of matching learning modules to the user. | To provide users with a list of similar training modules. |
| 412-Browse Similar Training Modules | *Needs adaptation* | | Functional | Should have | Find More Results | Users should have an option to find more results. | To provide users with additional similar training module options. |
| 413-Communicate with the Course Provider | *Native* | | Functional | Must have | Submit Question Form | Users should be able to submit a form with a topic, question, and uploaded document. | To effectively communicate the user's query to the trainers. |
| 413-Communicate with the Course Provider | *Native* | | Non-Functional | Should have | Timely Notifications | The platform should send notifications in a timely manner. | To ensure timely communication between users and trainers. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 413-Communicate with the Course Provider | *Native* | | Functional | Should have | Provide Feedback | Users should be able to provide feedback on the answer. | To gauge and improve the quality of support. |
| 413-Communicate with the Course Provider | *Native* | | Functional | Must have | Receive Reply Notification for User | Users should receive a notification when a trainer replies. | To inform the user about the answer to their query. |
| 413-Communicate with the Course Provider | *Native* | | Functional | Must have | Receive Notification for Trainers | Trainers should receive a notification when a user asks a question. | To inform trainers about the user's query. |
| 413-Communicate with the Course Provider | *Native* | | Functional | Must have | Access Contact Option | Users should be able to select a contact training module provider option. | To initiate communication with the course provider. |
| 413-Communicate with the Course Provider | *Native* | | Functional | Must have | View FAQ | Users should be able to view a list of Frequently Asked Questions. | To possibly provide immediate answers to user's queries. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 413-Communicate with the Course Provider | *Native* | | Functional | Must have | Reply to Question | Trainers should be able to reply to the user's question. | To provide answers to the user's query. |
| Access Analytics | *Native* | | Functional | Must have | Access to Analytics Environment | Users should be able to click on the "analytics" button and access the analytics environment. | To allow users to access analytics data. |
| Access Analytics | *Needs adaptation* | | Constraints | Could have | Training Module Availability | The institution should be offering a training module on the platform. | To ensure that there is data for analytics. |
| Access Analytics | *Needs adaptation* | | Non-Functional | Should have | Reliable Data Presentation | The analytics data should be presented reliably and accurately. | To ensure that users can trust the analytics data. |
| Access Analytics | *Native* | | Functional | Must have | Access Specific Training Module Analytics | Users should be able to click on a training module and view various analytics related to that module. | To provide detailed analytics for each training module. |
| Access Analytics | *Native* | | Functional | Must have | View Training Module Overview | Users should be able to see an overview of the training modules they are assigned to. | To provide users with a summary of the training modules. |
| Access Dashboard | *Native* | | Functional | Must have | Dashboard Access | Allow users to access a dashboard showing an overview of their training modules | To provide a central location for users to view and manage their courses and related items. |
| Access Dashboard | *Native* | | Functional | Must have | Bookmarks Overview | Users should see an overview of all the sections they have bookmarked across various training modules. | To allow users to easily access and manage their bookmarks. |
| Access Dashboard | *Native* | | Functional | Must have | Completed Courses Overview | Users should see an overview of all training modules they have completed. | To allow users to easily access and manage their completed courses. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Access Dashboard | *Native* | | Functional | Must have | Training Modules Overview | Users should see an overview of all training modules they are currently enrolled in. | To allow users to easily access and manage their current training modules. |
| Access Dashboard | *Native* | | Functional | Must have | Favorites Overview | Users should see an overview of all training modules they have marked as favorites. | To allow users to easily access and manage their favorite training modules. |
| Add Favourite Course | *Native* | | Functional | Must have | Adding Course to Favourite List | Upon clicking the button, the course should be added to the user's favourite list. | To ensure that the system correctly adds the selected courses to the favourite list. |
| Add Favourite Course | *Native* | | Functional | Must have | Browse Courses | Users must be able to browse courses in the DCM. | To allow users to explore available courses. |
| Add Favourite Course | *Native* | | Functional | Must have | View and Edit Favourite List | Users should be able to view and edit their favourite list. | To allow users to manage their favourite courses. |
| Add Favourite Course | *Native* | | Constraints | Could have | User Authentication | Users must be logged into the DCM to add courses to their favourite list. | To ensure the security and personalization of the favourite list. |
| Add Favourite Course | *Native* | | Non-Functional | Should have | Response Time | The system should quickly add courses to the favourite list and show an appropriate confirmation. | To ensure the system is efficient and provides immediate feedback to the user. |
| Add Favourite Course | *Native* | | Non-Functional | Should have | Accessibility | The "Add to Favourite" button should be easily accessible and visible. | To ensure users can easily find and use the functionality. |
| Add Favourite Course | *Native* | | Functional | Must have | Add to Favourite Button | Each course listing must have an "Add to Favourite" button. | To facilitate users in adding courses to their favourite list. |
| Assign/remove user profiles | *Native* | | Functional | Must have | Editing Environment | The system should provide an editing environment for updating profile information. | To allow users to make necessary changes to the profiles. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Assign/remove user profiles | *Native* | | Functional | Must have | Manage User Profile Tab | The system must have a "Manage User Profile" tab. | To allow users to navigate to the profile management section. |
| Assign/remove user profiles | *Native* | | Constraints | Could have | User Access Rights | Users must have the right access to assign and remove profiles. | To ensure only authorized users can manage profiles. |
| Assign/remove user profiles | *Needs adaptation* | | Constraints | Could have | Line Manager Approval | Users can only assign or remove a profile after receiving approval from the line manager. | To ensure proper authorization and avoid unauthorized profile changes. |
| Assign/remove user profiles | *Native* | | Functional | Must have | Retrieve Profile | The system should retrieve and display the requested user profile. | To ensure users can view and manage the desired profiles. |
| Assign/remove user profiles | *Native* | | Functional | Must have | Search Profile | Users should be able to search for a profile by entering a name. | To facilitate the finding of specific user profiles. |
| Assign/remove user profiles | *Native* | | Functional | Must have | Profile Update Confirmation | The system should confirm that the profile has been updated. | To provide feedback to the user about the update status. |
| Communicate with Trainees | *Native* | | Functional | Must have | Send New Message to Class | Enable trainers to send new messages to the entire class. | To allow trainers to disseminate information to all trainees efficiently. |
| Communicate with Trainees | *Native* | | Functional | Must have | Formatting Options for Message | Provide formatting options for message content. | To enhance the presentation of the message. |
| Communicate with Trainees | *Needs adaptation* | | Functional | Must have | Notification for Missing Information | Notify trainers if any essential information is missing. | To ensure all necessary details are included in the message. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Communicate with Trainees | *Native* | | Functional | Must have | Select Course for Message | Allow trainers to select a specific course to send a message. | To ensure messages are sent to the intended recipients. |
| Communicate with Trainees | *Native* | | Functional | Must have | Send Message | Enable the message to be sent to all the trainees of a course. | To ensure the message reaches all intended recipients. |
| Communicate with Trainees | *Native* | | Constraints | Must have | Trainer Authentication | Allow only authenticated trainers to send messages. | To ensure the security and privacy of messages. |
| Communicate with Trainees | *Native* | | Functional | Must have | Access to Message Environment | Allow trainers to access a message environment. | To facilitate communication between trainers and trainees. |
| Communicate with Trainees | *Native* | | Functional | Must have | Store Sent Message | Ensure that sent messages are stored in the sent messages folder. | To keep a record of sent messages. |
| Communicate with Trainees | *Needs adaptation* | | Non-Functional | Should have | Timely Error Notifications | Provide timely error notifications for internet or server issues. | To keep the user informed about the system status and possible interruptions. |
| Communicate with Trainees | *Native* | | Functional | Must have | Input Subject and Message Content | Enable trainers to input the subject and content of the message. | To provide complete information in the message sent to trainees. |
| Configure Training Module Feedback | *Native* | | Functional | Must have | Access to Feedback Responses | The trainer should receive a notification and be able to access the feedback responses after the feedback period concludes. | To allow the trainer to review and analyze the feedback. |
| Configure Training Module Feedback | *Native* | | Functional | Must have | Feedback Form Configuration | The trainer should be able to configure both pre- and post-training module feedback forms. | To collect feedback from trainees about the training modules. |
| Configure Training Module Feedback | *Native* | | Constraints | Could have | Trainee Enrollment | Trainees must be enrolled in the training module for feedback forms to be sent. | To ensure that feedback forms are sent to relevant individuals. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Configure Training Module Feedback | *Needs adaptation* | | Constraints | Could have | Role-Based Access | Only users with a role that allows them to create training modules within the Institution can configure feedback forms. | To ensure that only authorized individuals can configure feedback forms. |
| Configure Training Module Feedback | *Needs adaptation* | | Non-Functional | Should have | Reliable Notification System | The trainer should reliably receive notifications regarding the availability of feedback responses. | To ensure that trainers are promptly informed about the availability of feedback responses. |
| Configure Training Module Feedback | *Native* | | Functional | Must have | Automatic Sending of Feedback Forms | The platform should automatically send feedback forms to enrolled trainees within the specified date range. | To ensure timely collection of feedback without manual intervention. |
| Configure Training Module Feedback | *Native* | | Functional | Must have | Feedback Form Customization | The trainer should be able to customize questions or select from predefined options for the feedback forms. | To tailor the feedback forms to the specific needs and concerns of the trainer. |
| Configure Training session Feedback | *Native* | | Functional | Must have | View Feedback Summary | Users must be able to view and analyze feedback summary. | To allow users to understand and analyze the feedback received. |
| Configure Training session Feedback | *Native* | | Functional | Must have | Enable Pre-Training Session Feedback Form | Users should have the option to enable a pre-training session feedback form. | To collect feedback from trainees before the training session. |
| Configure Training session Feedback | *Native* | | Functional | Must have | Specify Feedback Period | Users must be able to specify the feedback period. | To define the duration for sending and receiving feedback forms. |
| Configure Training session Feedback | *Native* | | Functional | Must have | Access to Feedback Environment | Users must be able to access a feedback environment. | To enable users to configure feedback forms. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Configure Training session Feedback | *Needs adaptation* | | Functional | Must have | Automatic Sending of Feedback Forms | System should automatically send feedback forms to enrolled trainees. | To ensure all trainees receive the feedback form. |
| Configure Training session Feedback | *Native* | | Constraints | Must have | User Authorization | Only authorized users should configure feedback forms. | To ensure security and relevance of feedback forms. |
| Configure Training session Feedback | *Native* | | Functional | Must have | Customize Feedback Questions | Users must be able to customize questions for the feedback form. | To ensure the feedback form is relevant and useful. |
| Configure Training session Feedback | *Native* | | Functional | Must have | Notification for Feedback Responses | Users should receive a notification for feedback responses. | To inform users that feedback responses are available for review. |
| Configure Training session Feedback | *Needs adaptation* | | Non-Functional | Should have | Timely Notifications | System should send timely notifications regarding feedback responses. | To keep users informed about the status of feedback responses. |
| Create institution user profiles | *Needs adaptation* | | Functional | Must have | Setting User Profile Information | The user should be able to set the new institution user profile's username, password, institution, role, and permissions. | To define the details and access level of the new user profile. |
| Create institution user profiles | *Needs adaptation* | | Functional | Must have | Create New Institution User Profile Tab | The system must have a "Create New Institution User Profile" tab. | To allow Institution Managers to navigate to the profile creation section. |
| Create institution user profiles | *Needs adaptation* | | Constraints | Could have | Institution Manager Rights | Institution Manager must have the necessary rights to create various user profiles in the DCM. | To ensure proper authorization and avoid unauthorized profile creation. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Create institution user profiles | *Needs adaptation* | | Functional | Must have | User Profile Information Authentication | The system should authenticate the information about the new user profile. | To ensure the validity and accuracy of the new user profile information. |
| Create institution user profiles | *Needs adaptation* | | Constraints | Could have | Authenticated List of Institution Members | Institution Manager must have an institutions' authenticated list of all members. | To ensure valid and accurate profile creation. |
| Create institution user profiles | *Needs adaptation* | | Functional | Must have | Editing Window for Profile Creation | The system should provide an editing window for creating a new institution user profile. | To facilitate the creation of new user profiles. |
| Create institution user profiles | *Needs adaptation* | | Functional | Must have | User Notification | The system should notify the new user that their profile has been created. | To inform the new user about their profile creation. |
| Create institution user profiles | *Needs adaptation* | | Functional | Must have | Profile Creation Confirmation | The system should confirm that the new user profile has been created. | To provide feedback to the Institution Manager about the creation status. |
| Create personal user profiles | *Native* | | Functional | Must have | Sign Up Button | The system must have a "Sign Up" button. | To allow users to navigate to the profile creation section. |
| Create personal user profiles | *Needs adaptation* | | Constraints | Could have | Institution Manager Rights | Institution Manager must have the necessary rights to create various user profiles in the DCM. | To ensure proper authorization and avoid unauthorized profile creation. |
| Create personal user profiles | *Needs adaptation* | | Functional | Must have | User Notification Email | The system should send a notification email to the user for email confirmation. | To ensure the user's email is valid. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Create personal user profiles | *Needs adaptation* | | Constraints | Could have | Authenticated List of Institution Members | Institution Manager must have an institutions' authenticated list of all members. | To ensure valid and accurate profile creation. |
| Create personal user profiles | *Native* | | Functional | Must have | User Profile Creation Form | The system should provide a form for entering personal details. | To gather necessary information for creating a user profile. |
| Create personal user profiles | *Native* | | Functional | Must have | User Notification | The system should notify the new user that their profile has been created. | To inform the new user about their profile creation. |
| Create personal user profiles | *Native* | | Functional | Must have | Profile Creation Confirmation | The system should confirm that the new user profile has been created. | To provide feedback to the user about the creation status. |
| Create personal user profiles | *Native* | | Functional | Must have | Submission of User Details | The user should be able to submit the form after filling it. | To submit the details for profile creation. |
| Create personal user profiles | *Needs adaptation* | | Functional | Must have | Email Confirmation | The user should be able to confirm their email. | To verify the email address of the user. |
| Creation of Training Sessions | *Needs adaptation* | | Functional | Must have | Availability within Training Module | Make the Training Session available within the Training Module for Trainees. | To allow Trainees to access the Training Session. |
| Creation of Training Sessions | *Native* | | Functional | Must have | Training Staff Association | Associate the Training Session instance with the Training Staff. | To assign responsibility for the Training Session. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Creation of Training Sessions | *Native* | | Functional | Must have | Form Filling | Enable the user to fill in a form with mandatory and other metadata fields for the Training Session. | To collect necessary information for the Training Session. |
| Creation of Training Sessions | *Native* | | Functional | Must have | Component Selection and Editing | Allow the user to choose components/resources and edit their properties. | To customize the Training Session. |
| Creation of Training Sessions | *Needs adaptation* | | Functional | Must have | Submission for Approval | Allow the user to submit the Training Session instance for approval by the Institution. | To ensure the Training Session meets institutional standards. |
| Creation of Training Sessions | *Native* | | Functional | Must have | Editing Environment | Provide an editing environment for creating a Training Session instance. | To facilitate the creation of a Training Session. |
| Creation of Training Sessions | *Needs adaptation* | | Functional | Must have | Approval Process | Enable the Institution manager to approve the Training Session. | To finalize the creation of the Training Session. |
| Creation of Training Sessions | *Needs adaptation* | | Functional | Must have | Notification to Institution Manager | Send a notification to the Institution manager for approval. | To inform the Institution manager of the pending Training Session. |
| Creation of Training Sessions | *Native* | | Functional | Must have | Notification to Trainer | Notify the Trainer about the approval and the unique ID. | To inform the Trainer of the successful creation of the Training Session. |
| Creation of Training Sessions | *Native* | | Functional | Must have | Identify Training Module | Allow user to identify and click on the Training Module where the Training Session is to be instantiated. | To initiate the process of creating a Training Session. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Creation of Training Sessions | *Native* | | Non-Functional | Should have | Data Consistency | Ensure the consistency of data between the Training Session and the Training Module. | To maintain data integrity. |
| Creation of Training Sessions | *Native* | | Constraints | Could have | User Permissions | The user must have the appropriate permissions to create a Training Session. | To maintain security and control over Training Session creation. |
| Creation of Training Sessions | *Native* | | Functional | Must have | Database Update | Update the corresponding database with Training Session details. | To maintain up-to-date records. |
| Creation of Training Sessions | *Native* | | Functional | Must have | Linking to Training Module | Link the approved Training Session to the corresponding Training Module. | To make the Training Session accessible within the Training Module. |
| Creation of Training Sessions | *Native* | | Non-Functional | Should have | Notification Clarity | Ensure clear and concise notifications for submission errors and approval status. | To provide clear communication to the user. |
| Creation of Training Sessions | *Native* | | Functional | Must have | Content Addition | Enable the user to add/upload initial content for the Training Session instance. | To provide content for the Training Session. |
| Creation of Training Sessions | *Needs adaptation* | | Functional | Must have | Generate Unique ID | Generate a unique ID for the Training Session upon approval. | To uniquely identify the Training Session. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| DCM module provider website integration | *Native* | | Constraints | Could have | Proper Integration | The integration should be well implemented, ensuring no broken links. | To ensure a seamless user experience. |
| DCM module provider website integration | *Native* | | Constraints | Could have | Up-to-Date Information | Module providers' website links should be up-to-date and working properly. | To avoid confusion and ensure the delivery of correct and relevant information. |
| DCM module provider website integration | *Native* | | Non-Functional | Should have | Security | Ensure that the links are secure. | To ensure user safety and data protection. |
| DCM module provider website integration | *Native* | | Functional | Must have | Clickable Links | The DCM should have clickable links directing to the module providers' websites. | To facilitate easy access to module providers' websites. |
| DCM module provider website integration | *Native* | | Functional | Must have | External Website Access | Users should be able to access additional information on module providers' websites. | To provide additional information to the users. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| DCM module provider website integration | *Native* | | Non-Functional | Should have | Loading Speed | The links should quickly redirect users to the respective websites. | To save users' time and ensure efficiency. |
| Edition of Training Sessions | *Needs adaptation* | | Functional | Must have | Temporary Backup | Temporarily store a copy of the current Training Session instance before making changes. | To allow for retrieval in case of rejection by Institution Manager. |
| Edition of Training Sessions | *Native* | | Functional | Must have | Editing Environment | Provide an editing environment for the user to make changes to the Training Session. | To enable the user to make necessary changes to the Training Session. |
| Edition of Training Sessions | *Native* | | Functional | Must have | Edit Option | Provide an option for the user to edit the selected Training Session. | To facilitate the editing of a Training Session. |
| Edition of Training Sessions | *Needs adaptation* | | Functional | Must have | Institution Manager Approval for Editing | Allow the Institution Manager to approve or reject the editing request. | To finalize the editing of the Training Session. |
| Edition of Training Sessions | *Needs adaptation* | | Functional | Must have | Notification to Institution Manager | Notify the Institution Manager about the editing request for approval. | To inform the Institution Manager of the pending editing request. |
| Edition of Training Sessions | *Native* | | Functional | Must have | Notification to Trainer | Notify the Trainer about the status of the editing request. | To inform the Trainer of the successful or unsuccessful editing of the Training Session. |
| Edition of Training Sessions | *Native* | | Functional | Must have | Identify Training Module and Session | The system should allow the user to identify and select the Training Module and Session for editing. | To initiate the process of editing a Training Session. |
| Edition of Training Sessions | *Native* | | Constraints | Could have | User Permissions | The user must have the appropriate permissions to edit a Training Session. | To maintain security and control over Training Session editing. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Edition of Training Sessions | *Native* | | Functional | Must have | Final Update | Update the Training Session in the system and database upon approval. | To maintain up-to-date records. |
| Edition of Training Sessions | *Native* | | Non-Functional | Should have | Notification Clarity | Ensure clear and concise notifications for editing requests and status. | To provide clear communication to the user. |
| Elimination of Training Sessions | *Needs adaptation* | | Functional | Must have | Temporary Store | Temporarily store the Training Session instance upon deletion request. | To allow for retrieval in case of rejection by Institution Manager. |
| Elimination of Training Sessions | *Needs adaptation* | | Functional | Must have | Delete Option | Provide an option for the user to delete the selected Training Session. | To facilitate the deletion of a Training Session. |
| Elimination of Training Sessions | *Needs adaptation* | | Functional | Must have | Institution Manager Approval for Deletion | Allow the Institution Manager to approve or reject the deletion request. | To finalize the deletion of the Training Session. |
| Elimination of Training Sessions | *Needs adaptation* | | Functional | Must have | Notification to Institution Manager | Notify the Institution Manager about the deletion request for approval. | To inform the Institution Manager of the pending deletion request. |
| Elimination of Training Sessions | *Native* | | Functional | Must have | Notification to Trainer | Notify the Trainer about the status of the deletion request. | To inform the Trainer of the successful or unsuccessful deletion of the Training Session. |
| Elimination of Training Sessions | *Native* | | Functional | Must have | Identify Training Module and Session | The user should be able to identify and select the Training Module and Session for deletion. | To initiate the process of deleting a Training Session. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Elimination of Training Sessions | *Native* | | Constraints | Could have | User Permissions | The user must have the appropriate permissions to delete a Training Session. | To maintain security and control over Training Session deletion. |
| Elimination of Training Sessions | *Native* | | Functional | Must have | Final Deletion | Delete the Training Session from the system and update the database upon approval. | To maintain up-to-date records. |
| Elimination of Training Sessions | *Native* | | Functional | Must have | Confirmation Prompt | Display a confirmation message to ensure the user wants to delete the selected Training Session. | To prevent accidental deletion of Training Sessions. |
| Elimination of Training Sessions | *Native* | | Non-Functional | Should have | Notification Clarity | Ensure clear and concise notifications for deletion requests and status. | To provide clear communication to the user. |
| Enrolment in a Training Session Instance | *Needs adaptation* | | Functional | Must have | Temporary Storage of Request | Temporarily store the enrolment request and notify the Institution Manager. | To allow for retrieval in case of rejection by Institution Manager. |
| Enrolment in a Training Session Instance | *Native* | | Functional | Must have | Enrolment Option | Provide an option for the user to enroll in the selected Training Session. | To facilitate the enrolment in a Training Session. |
| Enrolment in a Training Session Instance | *Needs adaptation* | | Functional | Must have | Institution Manager Approval for Enrolment | Allow the Institution Manager to approve or reject the enrolment request. | To finalize the enrolment in the Training Session. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Enrolment in a Training Session Instance | *Native* | | Functional | Must have | Notification to Trainee | Notify the Trainee about the status of the enrolment request. | To inform the Trainee of the successful or unsuccessful enrolment in the Training Session. |
| Enrolment in a Training Session Instance | *Native* | | Functional | Must have | Identify Training Module and Session | The system should allow the user to identify and select the Training Module and Session for enrolment. | To initiate the process of enrolment in a Training Session. |
| Enrolment in a Training Session Instance | *Native* | | Constraints | Could have | User Permissions | The user must have the appropriate permissions to enroll in a Training Session. | To maintain security and control over Training Session enrolment. |
| Enrolment in a Training Session Instance | *Native* | | Functional | Must have | Final Update | Update the Training Session and related databases upon approval. | To maintain up-to-date records. |
| Enrolment in a Training Session Instance | *Native* | | Non-Functional | Should have | Notification Clarity | Ensure clear and concise notifications for enrolment requests and status. | To provide clear communication to the user. |
| Evaluation of Training Sessions | *Native* | | Functional | Must have | Evaluation Asset Activation | Enable access to the activated evaluation asset for the user to complete. | To allow the user to complete the evaluation asset. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Evaluation of Training Sessions | *Native* | | Functional | Must have | Automatic Evaluation | Conduct automatic evaluation if pre-defined by the trainer. | To automate the evaluation process when chosen. |
| Evaluation of Training Sessions | *Native* | | Functional | Must have | Manual Evaluation Notification | Notify the trainer for manual evaluation when necessary. | To ensure manual evaluation is conducted when required. |
| Evaluation of Training Sessions | *Needs adaptation* | "function properly" | Constraints | Could have | Evaluation Mode Availability | The chosen evaluation mode (automatic or manual) should function properly. | To ensure the accuracy and functionality of the evaluation process. |
| Evaluation of Training Sessions | *Native* | | Functional | Must have | User Notification | Notify the user about the final result of the evaluation. | To inform the user about the evaluation results. |
| Evaluation of Training Sessions | *Native* | | Functional | Must have | Access to Training Module and Session | The system should allow the user to identify and access the Training Module and Session for evaluation. | To initiate the evaluation process. |
| Evaluation of Training Sessions | *Native* | | Functional | Must have | Grade Assignment and Storage | Assign and store grades in the database. | To keep a record of grades for evaluations. |
| Evaluation of Training Sessions | *Native* | | Non-Functional | Should have | Timely Notifications | Ensure timely notifications for evaluation status and results. | To provide clear and timely communication to the user. |
| Evaluation of Training Sessions | *Native* | | Functional | Must have | Submission of Evaluation Asset | Allow users to submit the completed evaluation asset for evaluation. | To submit the evaluation asset for grading. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Invitation to Training Sessions | *Native* | | Functional | Must have | Access to Training Module and Session | The system must allow the Trainer to access the Training Module and Session links. | To enable the Trainer to navigate to the specific Training Session for adding new users. |
| Invitation to Training Sessions | *Needs adaptation* | "external users" | Functional | Must have | Add Internal and External Users | The system must provide options to add both internal and external users to the Training Session. | To ensure that all types of users can be added to the Training Session. |
| Invitation to Training Sessions | *Needs adaptation* | | Functional | Must have | Notification to Institution Manager | The system should notify the institution manager for the approval of the new user addition. | To ensure that the new user addition is approved by the relevant authority. |
| Invitation to Training Sessions | *Native* | | Functional | Must have | Manage Security Properties | The system must enable the management of security and visibility properties for the new user. | To ensure that the new user has the appropriate access rights to the Training Session. |
| Invitation to Training Sessions | *Native* | | Functional | Must have | Add External User Information | The system must allow the entering of external user information. | To facilitate the addition of external users to the Training Session. |
| Invitation to Training Sessions | *Native* | | Functional | Must have | Search for Internal Users | The system must enable the searching of internal users within the platform's database. | To facilitate the addition of internal users to the Training Session. |
| Invitation to Training Sessions | *Native* | | Functional | Must have | Update Databases | The system must update the related databases after the new user is added to the Training Session. | To keep the databases updated with the latest information. |
| Invitation to Training Sessions | *Native* | | Non-Functional | Should have | Security | The system should ensure that the security and visibility conditions for the new users are maintained. | To safeguard the information and resources of the Training Session. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Join forum | *Native* | | Functional | Must have | Search Functionality | Users should be able to search the group to check if a question/topic/issue of concern has already been posted. | To avoid duplication and ensure efficient use of forum resources. |
| Join forum | *Needs adaptation* | | Constraints | Could have | User Authentication | Only users enrolled in a partner institution and logged into the DCM should be able to join the forum. | To ensure security and authenticity of forum participants. |
| Join forum | *Native* | | Constraints | Could have | Availability of Forums | Forums or discussion boards and well-defined categories should have already been created within the DCM. | To ensure that the infrastructure for forum participation is available. |
| Join forum | *Native* | | Functional | Must have | Moderation | The forum moderator should be able to moderate and approve or disapprove the new question. | To ensure the quality and relevance of the forum content. |
| Join forum | *Native* | | Functional | Must have | Post Creation | Users should be able to create and post a new question. | To ensure users can easily post their queries or topics for discussion. |
| Join forum | *Native* | | Functional | Must have | Join Forum Button | Users should be able to see and click a button to join one or more groups of interest. | To facilitate user participation in forums. |
| Join forum | *Native* | | Functional | Must have | Guideline Presentation | First-time users should be presented with a page containing forum or community guidelines. | To inform users about the guidelines and ensure compliance. |
| Join forum | *Native* | | Non-Functional | Should have | Notification System | Users should receive timely notifications regarding the status of their posts and replies. | To keep users informed and engaged. |
| Like course | *Needs adaptation* | | Non-Functional | Should have | Immediate Feedback | Upon liking a course, users should receive immediate visual feedback. | To confirm to the user that their like has been registered. |
| Like course | *Needs adaptation* | | Functional | Must have | Like Button | Users should be able to see and click a "like" button next to each course listed in the DCM. | To allow users to express their preference for a course. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Like course | *Needs adaptation* | | Constraints | Could have | User Authentication | Only users who are logged into the DCM can like a course. | To ensure that only authenticated users can interact with the course listings. |
| Like course | *Native* | | Constraints | Could have | Course Availability | Courses must have been created and populated in the DCM database. | To ensure that there are courses available for users to like. |
| Like course | *Needs adaptation* | | Functional | Must have | Like Count | The number of likes for each course should be displayed below each course. | To provide feedback to users and course creators about the popularity of a course. |
| Make enquiry | *Needs adaptation* | "email" | Functional | Must have | Confirmation Notification | Users should receive a confirmation notification via email after submitting an enquiry. | To acknowledge the receipt of the user's enquiry. |
| Make enquiry | *Needs adaptation* | "immediately" | Non-Functional | Should have | Response Time | Users should receive a confirmation notification immediately after enquiry submission. | To ensure immediate feedback to the user regarding the enquiry submission. |
| Make enquiry | *Native* | | Functional | Must have | Submit Enquiry | Users should be able to complete and submit the enquiry form. | To ensure users can easily send their enquiries. |
| Make enquiry | *Native* | | Constraints | Could have | Form Availability | An enquiry form must be available as part of the Contact Us page of the DCM. | To ensure users have a platform to make enquiries. |
| Make enquiry | *Native* | | Functional | Must have | Enquiry Form | The DCM should have an enquiry form as part of the Contact Us page. | To facilitate users in making enquiries about the CyberSecPro training programme. |
| Manage user profiles | *Needs adaptation* | | Functional | Must have | Access to Manage User Profile | The Institution Manager should have access to manage user profiles. | To allow authorized personnel to manage user profiles. |
| Manage user profiles | *Needs adaptation* | | Functional | Must have | Edit User Profile | The system should display an editing environment for the Institution Manager to update user profile information. | To allow the updating of user profile information. |
| Manage user profiles | *Needs adaptation* | | Constraints | Could have | Access Rights | The Institution Manager must have the right access to update user profiles. | To ensure that only authorized personnel can update user profiles. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Manage user profiles | *Needs adaptation* | | Functional | Must have | Retrieve User Profile | The system should allow the Institution Manager to retrieve a user profile by entering the name. | To facilitate the retrieval of user profiles for editing. |
| Manage user profiles | *Needs adaptation* | | Functional | Must have | Confirmation of Update | The system should display a confirmation that the profile has been updated. | To provide feedback to the Institution Manager about the status of the update. |
| Provide realtime online customer support | *Needs adaptation* | chat / chatbot | Functional | Must have | Connect with Agent | After submitting the form, the user should be connected with the next available live customer service agent. | To ensure the user receives timely assistance. |
| Provide realtime online customer support | *Needs adaptation* | | Functional | Should have | Queue Management | If all agents are busy, place the user in a queue. | To manage user expectations and ensure all requests for assistance are handled. |
| Provide realtime online customer support | *Needs adaptation* | | Functional | Must have | User Registration | The system should display a registration form requiring name and email for feedback service management. | To collect necessary information from the user for communication and feedback. |
| Provide realtime online customer support | *Needs adaptation* | | Functional | Must have | Initiate Contact | The system should allow the user to initiate contact with a live agent by clicking a messaging button. | To enable users to easily request assistance. |
| Provide realtime online customer support | *Needs adaptation* | | Non-Functional | Should have | Response Time | The system should connect the user to a live agent with minimal delay. | To enhance user satisfaction by providing timely assistance. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Provide realtime online customer support | *Needs adaptation* | | Non-Functional | Should have | Data Security | The user's registration details and communication history should be securely stored and transmitted. | To ensure the privacy and security of user information. |
| Provide Training module Feedback | *Needs adaptation* | | Functional | Must have | Feedback Form Access | Trainees should be able to access the feedback form by clicking on the notification. | To enable trainees to provide feedback easily. |
| Provide Training module Feedback | *Native* | | Functional | Must have | Feedback Submission | Trainees should be able to submit their feedback. | To ensure feedback is collected. |
| Provide Training module Feedback | *Needs adaptation* | | Non-Functional | Should have | Timely Notifications | The platform should send notifications in a timely manner. | To ensure trainees have sufficient time to provide feedback. |
| Provide Training module Feedback | *Native* | | Functional | Must have | Feedback Form Structure | The feedback form should allow trainees to evaluate various aspects. | To gather comprehensive feedback from trainees. |
| Provide Training module Feedback | *Native* | | Functional | Must have | Notification for Feedback Form | The platform should send a notification to the trainees about the availability of a feedback form. | To inform trainees about the opportunity to provide feedback. |
| Provide Training module Feedback | *Native* | | Functional | Must have | Update Trainer Dashboard | The system should update the trainer’s feedback dashboard. | To keep trainers informed about the feedback. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Provide Training module Feedback | *Native* | | Constraints | Could have | Feedback Period | Feedback can only be provided within a specified period. | To maintain a structured feedback collection process. |
| Provide Training module Feedback | *Needs adaptation* | | Functional | Must have | Feedback Storage | The platform should securely store the feedback. | To maintain the integrity and confidentiality of feedback. |
| Provide Training Session Feedback | *Native* | | Functional | Must have | Access to Feedback Form | Trainees must be able to access the feedback form by clicking on the notification. | To enable trainees to provide feedback easily. |
| Provide Training Session Feedback | *Native* | | Functional | Must have | Feedback Form Submission | Trainees must be able to submit their feedback. | To ensure feedback is collected. |
| Provide Training Session Feedback | *Needs adaptation* | | Non-Functional | Should have | Timely Feedback Form Availability | The system should ensure that the feedback form is available to trainees within the specified feedback period. | To ensure trainees have sufficient time to provide feedback. |
| Provide Training Session Feedback | *Native* | | Functional | Must have | Feedback Form Structure | The feedback form should allow trainees to evaluate various aspects. | To gather comprehensive feedback from trainees. |
| Provide Training Session Feedback | *Native* | | Functional | Must have | Notification for Feedback Form | The platform must notify trainees about the availability of a feedback form. | To inform trainees about the opportunity to provide feedback. |
| Provide Training Session Feedback | *Needs adaptation* | | Functional | Must have | Updating Trainer Dashboard | The system must update the trainer's feedback dashboard. | To keep trainers informed about the feedback. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Provide Training Session Feedback | *Needs adaptation* | | Constraints | Could have | Limited Feedback Period | Trainees can only provide feedback within a certain period. | To maintain a structured feedback collection process. |
| Provide Training Session Feedback | *Native* | | Functional | Must have | Storing Feedback | The system must securely store the feedback. | To maintain the integrity and confidentiality of feedback. |
| React to User Review | *Needs adaptation* | | Functional | Must have | Reply to Review | Enable trainers to reply to specific user reviews. | To allow trainers to address specific comments or concerns raised in the reviews. |
| React to User Review | *Needs adaptation* | | Functional | Must have | User Review Feedback | Allow trainers to react to user reviews. | To enable trainers to respond to the feedback given by trainees, ensuring clarity and resolution of issues. |
| React to User Review | *Needs adaptation* | | Supplemental | Could have | User Interface | Provide a user-friendly interface for navigating and responding to reviews. | To ensure ease of use and efficiency for trainers in managing and responding to user reviews. |
| React to User Review | *Needs adaptation* | | Non-Functional | Should have | Notification | Send a notification to the user who left the original review after the trainer posts a response. | To inform the users about the trainer's response to their reviews. |
| React to User Review | *Needs adaptation* | | Functional | Must have | Review Listing | Display a list of user reviews for the trainer’s training module/session. | To provide trainers with an overview of the feedback received from trainees. |
| Review of Training Session Evaluations | *Needs adaptation* | | Functional | Must have | Display Overall Status and Scores | The system must display the overall status of the Training Session, each evaluation asset, and each Trainee along with their respective scores. | To provide a comprehensive overview of the Training Session evaluations to the Trainer. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Review of Training Session Evaluations | *Native* | | Functional | Must have | Review Training Session Evaluations | The system should enable the Trainer to review the Training Session evaluations. | To allow the Trainer to analyze the evaluation results of the Training Session. |
| Review of Training Session Evaluations | *Native* | | Functional | Must have | Access to Training Module and Session | The system must allow the Trainer to access the Training Module and Session links. | To enable the Trainer to navigate to the specific Training Session for reviewing evaluations. |
| Review of Training Session Evaluations | *Needs adaptation* | | Non-Functional | Should have | Reliable Data Display | The system should ensure that the displayed data is accurate and reliable. | To ensure the Trainer can make informed decisions based on the displayed data. |
| Get Detailed Training Session Result | *Native* | | Functional | Must have | Display Training Session Environment | Provide the environment for the specific Training Session to the user. | To facilitate the user in navigating to the specific Training Session. |
| Get Detailed Training Session Result | *Native* | | Functional | Must have | Access to Training Module Link | The system should allow the user to access the Training Module where the Training Session was instantiated. | To initiate the process of reviewing Training Session results. |
| Get Detailed Training Session Result | *Native* | | Functional | Must have | Show Training Session Results | Allow the user to view the results of the specific Training Session. | To provide the user with the necessary information regarding their performance in the Training Session. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Schedule Training Sessions | *Native* | | Functional | Must have | Add/Edit Schedule | The system should enable the Trainer to add or edit one or more schedules for a particular Training Session. | To allow the Trainer to set the schedules for the Training Session. |
| Schedule Training Sessions | *Native* | | Functional | Must have | Access to Training Module and Session | The system must allow the Trainer to access the Training Module and Session links. | To enable the Trainer to navigate to the specific Training Session for scheduling. |
| Schedule Training Sessions | *Needs adaptation* | | Functional | Must have | Submission for Approval | The system must allow the Trainer to submit the new schedule for approval by the Institution. | To ensure the schedule is approved and validated by the Institution before being finalized. |
| Schedule Training Sessions | *Needs adaptation* | | Constraints | Could have | Institution Approval | The new schedule must be approved by the Institution before being finalized. | To ensure the validity and acceptance of the new schedule. |
| Schedule Training Sessions | *Needs adaptation* | | Non-Functional | Should have | Reliable Notification System | The system should send reliable notifications to both the Trainer and the manager of the Institution regarding the approval status. | To keep all parties informed about the schedule approval status. |
| Search Engine for Training Sessions | *Native* | | Functional | Must have | Search Options | Provide simple and advanced search options for finding training sessions. | To facilitate effective searching. |
| Search Engine for Training Sessions | *Native* | | Functional | Must have | Access to Search Engine | The system should allow users to access the search engine for training sessions. | To initiate the search process. |
| Search Engine for Training Sessions | *Needs adaptation* | | Functional | Must have | Access to Training Session Information | Allow users to access more information about a training session by clicking on the associated link. | To provide detailed information about a training session. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Search Engine for Training Sessions | *Needs adaptation* | | Functional | Must have | Display Search Results | List the found training sessions with relevant information and links. | To provide users with the search results. |
| Set Bookmark | *Native* | | Non-Functional | Should have | Visual Indication | The platform should provide a clear visual indication that a bookmark has been set. | To clearly inform the user about the bookmark status. |
| Set Bookmark | *Native* | | Functional | Must have | Bookmark Setting Option | The platform should display a bookmark setting option within the learning content interface. | To enable users to easily set bookmarks. |
| Set Bookmark | *Native* | | Constraints | Must have | Platform Compatibility | The training module should be hosted on the platform. | To ensure the functionality of bookmarks. |
| Set Bookmark | *Native* | | Functional | Must have | Bookmark Acknowledgment | The platform should acknowledge the setting of a bookmark. | To provide feedback to the user about the action. |
| Set Bookmark | *Native* | | Functional | Must have | Access to Bookmark | The trainee should be able to access the bookmarked section at a later time. | To utilize the bookmark functionality effectively. |
| Share Participation | *Needs adaptation* | | Functional | Must have | Customize Post | Trainees should be able to customize the post. | To allow personalization of the shared post. |
| Share Participation | *Needs adaptation* | | Functional | Must have | Display Share Option | The platform should display a sharing option when a milestone is completed. | To enable users to share their achievements. |
| Share Participation | *Needs adaptation* | | Non-Functional | Should have | Quick Redirection | The platform should quickly redirect to social media platforms. | To ensure a smooth and efficient process. |
| Share Participation | *Needs adaptation* | | Constraints | Must have | Social Media Integration | The platform should be integrated with social media platforms. | To facilitate sharing on various platforms. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Share Participation | *Needs adaptation* | | Functional | Must have | Redirect to Social Media | The platform should redirect to the selected social media platform. | To facilitate the sharing process. |
| Share Participation | *Needs adaptation* | | Functional | Must have | Provide Social Media Options | The platform should provide different social media platforms for sharing. | To give users options for sharing achievements. |
| Share Participation | *Needs adaptation* | | Functional | Must have | Prefilled Post | The platform should provide a prefilled post for sharing. | To make the sharing process easier and consistent. |
| Share Participation | *Needs adaptation* | | Functional | Must have | Confirmation of Sharing | The platform should confirm successful sharing. | To notify the user of the successful action. |