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

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

CyberSecPro

D5.1
Evaluation Methodology

Document Identification	
Due date	2025-03-31
Submission date	2024-07-18
Version	1.0

Related WP	WP5	Dissemination Level	PU
Lead Participant	ACEEU	Lead Author	Prof. Dr Thorsten Kliewe (ACEEU)
Contributing Participants	COFAC, UPRC, UMA, MAG, LAU	Related Deliverables	D3.1, D3.3, D5.2, D6.2, D6.3, D6.4, D6.5

Abstract:

CyberSecPro (D5.1) details the evaluation methodology developed to assess satisfaction levels among trainers and trainees, as well as to evaluate MOOCs and training materials through peer-review processes. Unlike earlier surveys within the project, this approach is purpose-driven and tailored to capture experiential feedback rather than technical competencies. The report outlines the tools and strategies used for collecting and analysing both quantitative and qualitative data, emphasising user satisfaction, content relevance, and perceived effectiveness. By distinguishing its objectives from previous assessments, D5.1 establishes a nuanced framework that supports continuous improvement through stakeholder-driven insights. Recommendations also guide future analysis and data use to ensure CyberSecPro's training activities remain engaging, relevant, and aligned with participant expectations across the EU cybersecurity education landscape.

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

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

Executive Summary

The CyberSecPro Deliverable 5.1 presents the evaluation methodology designed to assess the quality, usability, and impact of training activities within the CyberSecPro project. It focuses on evaluating learner and trainer satisfaction, and the post-development review of MOOCs, all grounded in recognised standards and quality frameworks relevant to (cybersecurity) education.

Methodology: To develop Deliverable D5.1, a structured process was applied to:

- Review over 20 existing evaluation frameworks and initiatives from cybersecurity and online education sectors, including those by CyberSec4Europe, ENQA, and OpenupEd.
- Define technical, pedagogical, and business KPIs to assess training activities & MOOCs.
- Develop modular evaluation instruments embedded in the CSP Admin Portal, enabling trainers and providers to collect both quantitative and qualitative feedback.
- Establish processes for structured data collection, analysis, visualisation, and revision, supported by secure, centralised infrastructure.
- Outline benchmarking mechanisms for internal comparison and external transparency.

This work aligns with Task 5.1 "Evaluation Methodology Design" and informs subsequent evaluation activities under Task 5.2. It interfaces closely with WP3 (Training Development), WP4 (Training Implementation), and WP6 (Dissemination and Exploitation).

Findings and outcomes: Key outcomes from this deliverable include:

- A comprehensive, multi-level evaluation methodology that incorporates feedback loops from both trainees and trainers.
- Detailed KPI matrices and customizable survey templates to ensure consistency across diverse training formats.
- Post-development MOOC evaluation tools based on CyberSec4Europe's quality criteria, supporting self-assessment and compliance.
- Planning guidelines for data analysis, evaluation logistics, and role assignments to ensure smooth implementation across partners.
- Benchmarking strategies, enabling both intra-project analysis and public-facing comparisons for broader sector learning.

Conclusion: CyberSecPro Deliverable 5.1 marks a critical milestone in the project's quality assurance strategy. By providing a robust evaluation framework tailored to the needs of cybersecurity training, it supports both the continuous improvement of learning experiences and the long-term recognition of CyberSecPro as a reference point for excellence in the field. Through its flexible yet structured tools and processes, D5.1 lays the groundwork for systematic evaluation, meaningful benchmarking, and sustained educational impact.

Document Information

Contributors

Name	Beneficiary
Prof. Dr Thorsten Kliewe	ACEEU
Pamela Paula Maldini	ACEEU
Jeldo Meppen	ACEEU
Dr Lina Landinez	ACEEU
Aventia Wilona	ACEEU
Adekola Ashonibare	ACEEU
Dimitrios Koutras	UPRC
Cristina Alcaraz	UMA
Paulinus Ofem	LAU
Spiros Borotis	MAG
George Kliafas	MAG

Reviewers

Name	Beneficiary
Daniel Silveira	COFAC (As WP leader)
Ric Lugo	Taltech
Christos Douligeris	UPRC

History

Version	Date	Contributor(s)	Comment(s)
0.10	2025-12-16	Daniel Silveira (COFAC)	Initial table of contents
0.11	2025-12-22	Prof. Dr Thorsten Kliewe (ACEEU)	Adapted table of contents
0.20	2025-04-01	Prof. Dr Thorsten Kliewe (ACEEU), Pamela Paula Maldini (ACEEU), Jeldo Meppen (ACEEU), Dr Lina Landinez (ACEEU), Aventia Wilona (ACEEU), Adekola Ashonibare (ACEEU)	Initial internal draft based on the early outline.
0.30	2025-04-28	Prof. Dr Thorsten Kliewe (ACEEU), Pamela Paula Maldini (ACEEU), Daniel Silveira (COFAC)	Incorporated feedback from the WP5 leader during early development.
0.31	2025-04-31	Prof. Dr Thorsten Kliewe (ACEEU)	Integrated input from WP5 partners collected during regular meetings.
0.32	2025-05-15	Prof. Dr Thorsten Kliewe (ACEEU), Pamela Paula Maldini (ACEEU)	Revised based on ongoing WP5 feedback and internal discussion.
0.40	2025-05-18	Prof. Dr Thorsten Kliewe (ACEEU), Jeldo Meppen (ACEEU), Daniel Silveira (COFAC)	Version prepared for broader consortium review and shared for formal internal feedback.
0.5	2025-06-20	Prof. Dr Thorsten Kliewe (ACEEU), Jeldo Meppen (ACEEU)	Revised following peer review by Daniel Silveira (received 2025-06-19).
0.6	2025-06-22	Prof. Dr Thorsten Kliewe (ACEEU), Jeldo Meppen (ACEEU)	Updated following peer review by Ric Lugo (received 2025-06-21).
0.6	2025-06-03	Ahad Niknia (GUF)	High level review and check
0.7	2025-07-04	Prof. Dr Thorsten Kliewe (ACEEU), Jeldo Meppen (ACEEU)	Revised based on formatting feedback from GUF (received 2025-07-03).
0.8	2025-07-16	Prof. Dr Thorsten Kliewe (ACEEU), Jeldo Meppen (ACEEU), Dr Lina Landinez (ACEEU)	Final revision after peer review by Christos Douligeris (received 2025-07-16).

1.0	2025-07-17	Ahad Niknia (GUF)	Final review, check, improvement, preparation and submission process
1.1	2025-07-18	Jeldo Meppen (ACEEU)	Final formatting adaptations, grammar check
1.2	2025-07-17	Md Arman Khan (GUF)	Final review, check, improvement, preparation and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AI**	Artificial Intelligence
C	**CEF**	Contextualized Evaluation Framework
	CLAT	Collaborative Learning with Advanced Technologies
	CMF	Common Micro-Credential Framework
	CSP	CyberSecPro
D	**DBR**	Design-Based Research
	DCM	Digital Curriculum Management
E	**ECTS**	European Credit Transfer and Accumulation System
	EMC-LM	European MOOC Consortium - Labour Markets
	EMMA	European Multiple MOOC Aggregator
	ENQA	European Association for Quality Assurance in Higher Education
	EQF	European Qualifications Framework
	ESG	Standards and Guidelines for Quality Assurance
	EU	European Union
	EU IA Act	European Union Artificial Intelligence Act
	GDPR	General Data Protection Regulation
I	**ICT**	Information and Communication Technologies
	IDE	Integrated Development Environment
	IoT	Internet of Things
	ISM	Interpretive Structural Modelling
	ISO	International Organization for Standardization
K	**KPI**	Key Performance Indicator
L	**LIS**	Library and Information Science
	LLM	Large Language Model
M	**MEF**	MOOC Evaluation Framework

	MOOC	Massive Open Online Course
O	**OER**	Open Educational Resources
	OLEF	Online Learning Environment Form
Q	**QA**	Quality Assurance
	QRF	Quality Reference Framework
R	**ROI**	Return on Investment
S	**STEM**	Science, Technology, Engineering, and Mathematics
U	**UDL**	Universal Design for Learning
	URL	Uniform Resource Locator
W	**WBL**	Work-Based Learning
	WP	Work Package

Glossary of Terms

B **Benchmarking**

Internal and external comparison of training performance across courses, time, and institutions.

C **CyberSecPro competence**

The ability to perform tasks on a cognitive or practical level; knowing how to do it.

CyberSecPro Dynamic Curriculum Management System

A Moodle/e-class based system to manage curriculum creation, updates, and compliance, responsive to market needs.

CyberSecPro knowledge areas

Based on frameworks like CyBoK, JRC, ECSF, and industry-academia cooperation reports.

CyberSecPro practical skill

The ability to apply knowledge and skills to achieve measurable results.

CyberSecPro sector-specific training modules

Modules tailored to the health, maritime, and energy sectors, co-designed with industry and HEIs based on real-world challenges.

CyberSecPro syllabus

A standardised document per module with learning outcomes, target audience, prerequisites, module outline, tools, materials, assessment methods, and estimated study time.

CyberSecPro training format

Delivery modes including on-demand, web-based, live online, in-person, and hybrid.

CyberSecPro training material

All resources used by trainers to deliver a module.

CyberSecPro training modules

Includes courses, mini-courses, lectures, exercises, hackathons, events, games, red/blue team sessions, summer schools, workshops, seminars, and crisis simulations.

CyberSecPro training programme

A set of training modules offered individually or as a package to complement existing training and address gaps between academic education and industry needs.

CyberSecPro training tools

Tools selected for delivering training modules (evaluation in T2.3).

F **Feedback Instruments**

Structured questionnaires to collect satisfaction and outcome data from trainees.

I **Impact Analysis Tools**

Tools for measuring long-term training effects and knowledge application.

Instructor Support

Availability and responsiveness of educators.

L **Learner Engagement**

Metrics like time spent, completion rates, and interaction.

Likert scale

A 7-point rating scale used in the evaluation surveys to measure satisfaction levels.

M **Multidimensional Evaluation**

Combining pedagogical, technical, and business-focused indicators.

N **Net Promoter Score**

A metric used in the evaluation to determine how likely a trainee is to recommend the learning experience or how likely a trainer is to recommend the CSP training materials.

P **Pedagogical Design**

Use of effective teaching practices aligned with outcomes.

Provider

An organization, institution, or platform that develops, hosts, and delivers Massive Open Online Courses (MOOCs). MOOC providers are responsible for the technical infrastructure, content delivery, and overall management of MOOCs.

R **Revised Bloom's Taxonomy**

Cognitive domain framework for classifying learning outcomes.

S **Social Interaction**

Opportunities for peer and instructor interaction.

S **SubMOOCs**

Smaller, stackable units forming modular training paths.

T **Trainer**

An individual responsible for guiding, facilitating, or instructing learners in a MOOC. A trainer may create content, moderate discussions, provide feedback, and support learners throughout the course. Trainers can be subject-matter experts, university professors, industry professionals, or instructional designers involved in developing and delivering the MOOC experience.

U **Usability Evaluations**

Tools to assess ease-of-use, accessibility, and learner experience on platforms.

1 Introduction

1.1 Background

In the rapidly evolving field of cybersecurity, ensuring the quality, relevance, and impact of training and education initiatives is paramount. As digital threats grow in complexity and scale, so does the demand for competent professionals equipped with up-to-date skills and knowledge. The CyberSecPro project, funded by the European Union under the DIGITAL-2021-SKILLS-01 call, addresses this challenge by developing advanced, modular, and sector-specific training programs. These programs aim to bridge the skills gap in key domains such as health, maritime, and energy, while supporting lifelong learning and professional upskilling across Europe.

At the core of CyberSecPro is the ambition to deliver high-quality, learner-centred education through MOOCs and micro credentials, tailored to real-world needs. However, the effectiveness of such efforts depends not only on the content delivered but also on the ability to rigorously evaluate their pedagogical value, usability, and long-term impact. Therefore, robust evaluation mechanisms are essential to ensure that the training materials and platforms are engaging, inclusive, and aligned with the expectations of learners, trainers, employers, and policymakers.

Deliverable D5.1 lays the foundation for this by presenting the project's overarching evaluation methodology. It responds to the increasing need for transparency, comparability, and continuous improvement in cybersecurity training, drawing from existing best practices in educational evaluation, instructional design, and digital learning analytics. It also reflects CyberSecPro's commitment to aligning with European quality assurance frameworks such as ENQA and the OpenupEd Quality Spectrum, as well as incorporating innovative approaches such as learner sentiment analysis and AI-enhanced feedback mechanisms.

By setting clear standards and processes for evaluation and benchmarking, this deliverable supports CyberSecPro's strategic goal of becoming a reference model for high-quality cybersecurity training in Europe. It also contributes to the broader EU digital education agenda by promoting data-informed decision-making and stakeholder engagement in training design, delivery, and improvement.

1.2 Purpose & Scope

The primary purpose of Task 5.1 and the respective Deliverable 5.1 (this deliverable) is to develop a robust evaluation and benchmarking methodology that effectively measures the performance, usability, impact, and overall quality of the CyberSecPro project's training outputs, particularly MOOCs developed in Task 4.1 as well as the implementation of the Training Modules developed in Task 3.4, 3.5 and 3.6. The scope includes identifying and detailing relevant KPIs, developing evaluation tools and instruments, and defining clear processes for systematic feedback collection from trainers and trainees. Additionally, this task aims to ensure alignment with established quality criteria specific to (cybersecurity) education. The deliverable will have built upon (not replicate) the quality criteria and expectations that have been set in D3.1 and D3.3, e.g. with respect to the design and development of the curriculum, the modules and the DCM.

1.3 Relation With Other WPs and Deliverables

This task closely interfaces with multiple other Work Packages (WPs) and deliverables:

- **WP2 (CyberSecPro professional programme analysis):** Leveraging KPIs and requirements defined in Task 2.3 as a baseline for usability evaluation.
- **WP3 (CyberSecPro Curricula Portfolio):** Utilising feedback mechanisms developed therein to inform continuous implementation and refinement strategies. Utilising criteria and standards/expectations defined in the curriculum, module and DCM design and development.
- **WP4 (Operating CyberSecPro Professional Training Program):** Direct evaluation of operation of the training modules, providing quality assurance and recommendations for improvement.
- **WP6 (Dissemination, Exploitation, Sustainability and Market Take up):** The results of the evaluation will finally be used for dissemination (e.g. quotes) and exploitation/sustainability (e.g. scaling modules that are evaluated positively)

1.4 Structure of the Report

This report is structured into eight main chapters, accompanied by annexes and references, to provide a comprehensive overview of the evaluation methodology developed under Task 5.1.

It begins with an introduction that outlines the background, purpose, scope, and methodological approach, as well as its connection to other work packages.

Chapter 2 presents an extensive review of existing evaluation frameworks and relevant initiatives in cybersecurity and other fields of education, highlighting key models and best practices that inform the CyberSecPro approach.

Chapter 3 defines the context and objectives of the evaluation within the project.

Chapters 4 and 5 detail the evaluation strategies for different components: training implementation (by trainees and trainers), training materials, and MOOCs, each including KPIs, instruments, and data processes.

Chapter 6 outlines the evaluation logistics, including timing, responsibilities, and recommendations for data analysis.

Chapter 7 addresses how the evaluation data will be used for both internal and external benchmarking.

The report concludes in Chapter 8 with a summary of findings and key contributions. Supporting references and annexes provide additional resources and documentation relevant to the evaluation design.

2 Existing Evaluation Frameworks and Relevant Initiatives

2.1 General and Cybersecurity-Related Frameworks and Initiatives

In this section, we present an overview of frameworks and initiatives that relate to the challenge of developing a solid evaluation framework for CyberSecPro. After presenting each framework/initiative, a blue box highlights the relevance for CyberSecPro. While each framework/initiative brings valuable insights, not all insights will finally be used, given the projects context and limitations (refer to Chapter 3), such as the trade-off between length/depth of the survey and survey responses.

For the purposes of the CyberSecPro project, our research places a primary—though not exclusive—focus on evaluation frameworks related to digital learning and MOOCs. This emphasis reflects several key considerations:

- The digital components embedded in nearly all module implementations within the project;
- The use of the CyberSecPro Dynamic Curriculum Management (DCM) system as an eLearning platform, along with the intention to make the learning materials available for self-paced learning beyond the project's duration;
- The widespread familiarity and application of traditional evaluation frameworks by consortium partners, in contrast to the relative lack of established and research-based evaluation criteria specifically tailored to digital learning and MOOCs.

This focus aims to address existing gaps and ensure that the evaluation methodology is aligned with the digital nature of the learning experience promoted by the project.

2.1.1 Evaluation Methodology Leveraging AI by Chan (2023)

In this study, Chan (2023) proposes a novel evaluation framework that leverages generative LLMs, specifically Claude+, Dragonfly, GPT-4, and Sage to assess and compare MOOC platforms across eight key dimensions. These eight key dimensions are content, pedagogical design, learner support, technology infrastructure, social interaction, learner engagement, instructor support, and cost-effectiveness. The aim is to investigate the consistency of these AI-based evaluations as a proxy for trustworthiness, drawing parallels to convergent validity in traditional psychometrics.

The core of the framework involves having AI models rate multiple MOOC platforms across standardised categories. These ratings are then statistically analysed to evaluate whether the AI models:

1. Show consistent differentiation across platforms (discrimination),
2. Systematically overrate or underrate certain dimensions (bias),
3. Correlate with one another across dimensions (consistency).

Only Claude+ and Dragonfly produced sufficiently complete and analysable datasets (31 MOOC platforms × 8 dimensions). The framework employs:

- Descriptive statistics (min, max, range, SD),
- Paired sample t-tests to check for systematic rating differences,
- Correlation coefficients to assess rating consistency across dimensions.

The framework uses eight key evaluation dimensions (criteria), drawn from established literature on MOOC success and quality. Each dimension is rated on a scale from 1 (worst) to 10 (best):

Table 1: Evaluation Methodology Leveraging AI by Chan (2023)

Dimension	Definition & Indicators
Content/Course Quality	Relevance, accuracy, instructional design, and assessment quality.
Pedagogical Design	Use of effective teaching methods, alignment of learning outcomes and assessments, and encouragement of active learning.
Learner Support	Availability of technical and academic support services throughout the course.
Technology Infrastructure	Platform reliability, uptime, speed, compatibility with devices, and security features.
Social Interaction	Opportunities for learner-instructor and peer-to-peer interaction and collaboration.
Learner Engagement	Metrics like time spent, interaction frequency, forum activity, and completion rates.
Instructor Support	Instructor availability, response quality and speed, and frequency of guided sessions.
Cost-Effectiveness	Relationship between course cost and benefits (ROI, accessibility, revenue generation).

The linkage/alignment of Chan (2023) methodology with CyberSecPro

Systematic, Multi-Dimensional Evaluation of MOOCs

Chan (2023) proposes a structured framework using eight key quality dimensions to evaluate MOOC platforms. This aligns well with CyberSecPro's aim to develop high-quality online learning experiences in cybersecurity. By applying these dimensions, CyberSecPro can benchmark its courses and platforms systematically, ensuring that they meet high standards of quality and learner satisfaction.

Scalable Use of AI for Evaluation

One innovative aspect of Chan's work is the use of generative AI robots (e.g., Claude+, Dragonfly) to automate evaluations based on real user feedback across the web. For CyberSecPro, which targets scalable delivery of microcredentials across Europe, this approach offers a cost-effective and timely way to gather feedback and insights from a wide learner base. It complements traditional evaluations (e.g., surveys) and supports ongoing quality assurance.

Focus on Learner-Centric Metrics

Several of the dimensions in Chan's framework, such as learner support, engagement, social interaction, and instructor responsiveness, focus on learner experience and outcomes. This resonates with CyberSecPro's mission to not just deliver content but to support learners effectively, improve retention, and foster meaningful skill development in cybersecurity.

Compatibility with Digital and AI Trends in Education

CyberSecPro operates in the fast-evolving landscape of digital learning and cybersecurity. By referencing a study that integrates AI into education evaluation, CyberSecPro positions itself as a forward-thinking, data-informed project that embraces innovation. This also aligns with broader EU digital education strategies.

2.1.2 Chickering and Gamson's Seven Principles and the Revised Bloom's Taxonomy (Bali, 2014)

Bali's (2014) paper draws on two key frameworks: Chickering and Gamson's Seven Principles for Good Practice in Undergraduate Education, and the revised version of Bloom's Taxonomy. The frameworks were not developed by Bali; they are classic models. Bali applied the frameworks to evaluate four MOOCs in which the author personally participated for these reasons:

- MOOCS were being questioned in terms of educational quality
- As MOOCs are based on university courses, the scholar chose traditional higher education pedagogical criteria to assess them

- Bali aimed to offer insights based on learner experiences, not institutional metrics

Bali analysed four MOOCs on Coursera, covering psychology, mathematics, nutrition, and health. The analysis combined observation of videos, quizzes, assignments, peer assessment, and forum discussions. The frameworks used for the analysis are described next, followed by an overview of the analysis results.

1. Chickering and Gamson's Seven Principles

Bali used these principles to assess good pedagogical practices. The principles include seven dimensions aimed at assessing the pedagogy of MOOCs as shown in Table 2.

Table 2: Chickering and Gamson's Seven Principles Based on Bali (2014)

Principle	Description or Indicators
Student-faculty contact	Frequent, meaningful interaction between students and instructors supports motivation, engagement, and learning outcomes.
Cooperation among students	Learning is enhanced when students collaborate, share ideas, and support each other through peer discussions or group tasks
Active learning	Students learn more effectively when they engage directly through doing, applying, and reflecting, rather than just passively absorbing content.
Prompt feedback	Timely responses help students understand what they know, where they need improvement, and how to progress.
Time on task	Effective learning requires managing time well; students benefit from clear timelines, consistent pacing, and support to stay focused.
High expectations	Challenging students with rigorous standards encourages them to strive for excellence and deeper learning.
Respect for diverse learning styles	Recognising and accommodating different abilities, backgrounds, and preferences make learning inclusive and effective.

2. Revised Bloom's Taxonomy

Bali revised Bloom's Taxonomy to assess the depth of learning and cognitive engagement. The dimensions of the revised taxonomy are described in Table 3.

Table 3: Revised Bloom's Taxonomy Based on Bali (2014)

Principle	Description or Indicators
Remembering	Recalling facts, definitions, or basic concepts from memory.
Understanding	Comprehending ideas or interpreting meaning; explaining concepts in your own words
Applying	Using learned material in new situations or practical contexts.
Analysing	Breaking down information into parts to explore relationships or patterns
Evaluating	Critically assessing information or arguments to make judgements or justify decisions.
Creating	Producing original work or combining elements in new, meaningful ways.

Bali (2014) suggests that the two frameworks are applicable to online courses in Psychology, Mathematics, Nutrition, and Health.

3. Bali's analysis results on the four courses

Table 4: Comparison of the Four Courses by Bali (2014)

Course	Psychology	Mathematics	Nutrition	Health
Length	12 weeks	8 weeks	5 weeks	8 weeks
Course provisions	Weekly video lectures and downloadable slides, readings, quizzes (3 attempts)	Weekly video minilectures, optional textbooks, weekly quizzes (multiple attempts, changing questions), two peer-reviewed assignments	Weekly video minilectures, optional readings, weekly quizzes (multiple attempts), four peer-reviewed assignments	Weekly video minilectures, optional readings, weekly quizzes (multiple attempts), weekly assignments (not peer-reviewed)
Flexibility	Changed quiz deadlines so that all quiz deadlines were end of course date	Strict deadlines	All quiz deadlines were end of course date; assignments had deadlines so that peer-review could be done in a timely manner; however, a second "track" was available that excluded assignments	All quiz and Assignment deadlines were end of course date
Strengths	Discussion forum provided space to discuss areas not covered in the course; instructor held online office hours	Students created their own study notes and shared them with others; Rigorous course	Discussion forum provided space to discuss areas not covered in the course; peer-reviewed assignments allowed one to create something by	Assignments were reflective and encouraged deep analysis of what was learned, applying it to one's individual context

			applying learning in the course, then to view and assess the work of others	
Weaknesses	Quizzes as only assessment; quizzes tested recall only; large number of students interested in certain aspects of the course that were not the instructor's focus	Strictness of deadlines; time requirements (but this was part of the Rigour)	Very laid back – almost felt like taking a class in a hobby, rather than a college course	No feedback on assignments at all

The linkage/alignment of Bali (2014) methodology with CyberSecPro

Pedagogical Evaluation Centred on Learning, Not Just Completion

Bali (2014) emphasises that MOOC evaluation should focus on pedagogical quality and learning outcomes, not just metrics like enrolment or completion rates. This aligns perfectly with CyberSecPro's objective to build courses that foster competency development in cybersecurity, not just participation. Bali's use of Chickering and Gamson's Seven Principles and Bloom's Taxonomy encourages CyberSecPro to centre its MOOC design around deep learning, engagement, and critical thinking, which are crucial for effective upskilling in a technical field like cybersecurity.

Learner-Centred and Inclusive Approach

Bali's approach underscores the importance of flexibility, accessibility, and respect for diverse learners, especially in a global, massive, and open learning environment. For CyberSecPro, which targets varied learners (in terms of geography, experience, and digital access), these values are key. Bali's reflections on addressing diverse talents, learner autonomy, and different learning styles offer practical guidance on how CyberSecPro can make its courses more inclusive e.g., offering transcripts, localised content, or low-bandwidth formats.

Scalable Yet Authentic Assessment Methods

The framework critiques superficial assessments and promotes higher-order, authentic assessments, such as reflective writing, peer-reviewed projects, or real-world applications. For CyberSecPro, this supports the integration of lab exercise, case studies, or reflective exercises that go beyond quizzes, helping ensure microcredentials signal real competence.

2.1.3 Contextualised Evaluation Framework

Douglas et al. (2018) present and apply the Contextualised Evaluation Framework (CEF) to assess how instructors evaluate and interpret the effectiveness of MOOCs, particularly in STEM. CEF was developed because traditional metrics (e.g., completion rates) fail to capture the complexity and learner diversity of MOOCs. The need for an evaluation model that reflects what instructors find useful for pedagogical improvement also informed the development of the framework.

The development of the CEF was based on the work of Scriven's (2015) Key Evaluation Checklist and Davidson's (2006) Genuine Evaluation and adapted to the MOOC environment. CEF is grounded in stakeholder values by emphasising the importance of evaluation based on what instructors and learners' value.

Table 5: Instructor Values in MOOC Evaluation Based on Douglas et al. (2018)

Values	Description or Indicators
Informal formative assessment	Real-time feedback, student presence, and non-automated insights into learner understanding.
Personal learning goal recognition	Want to know if learners meet their own goals, not just course-defined objectives.
In-depth qualitative feedback	Ratings and short reviews are insufficient; prefer rich, narrative feedback or interviews.
Detailed learner usage data	Data on video engagement, drop-off points, and quiz performance trends for course improvement.
Flexibility to adjust courses	Want insights that allow them to modify future iterations of the course meaningfully.
Evidence of impact	Seek confirmation that students not only completed the course but also understood and applied what they learned.

Table 6: Learner Values in MOOC Evaluation Based on Douglas et al. (2018)

Values	Description or Indicators
Flexibility in learning paths	Use MOOCs in diverse ways. Some watch a few videos; others complete the full course.
Achievement of personal goals	May not care about certification or grades; just gaining specific knowledge or skills.
Minimal formal pressure	Low-pressure, self-directed engagement over formal assessments.
Relevance to career or interests	Content that supports specific goals (e.g., job skills, curiosity, self-improvement).
Autonomy	Freedom to engage with materials as needed without rigid structures

Tables 5 and 6 align with the framework's core idea: evaluation must reflect the diverse intentions and values of those involved, rather than impose a single notion of success.

The linkage/alignment of Douglas (2018) methodology with CyberSecPro

Contextualized Evaluation Focused on Stakeholder Needs

Douglas et al. (2018) introduce the Contextualised Evaluation Framework, which emphasises evaluating MOOCs based on stakeholder values, including learners, instructors, and institutions. This is directly relevant to CyberSecPro, which must demonstrate that its courses meet employer needs, support learner goals, and provide institutional value. The framework's foundation in Scriven's Key Evaluation Checklist ensures that the evaluation is principled, comprehensive, and tailored to context, essential for a complex and dynamic field like cybersecurity.

Call for Rich, Actionable Learning Analytics

Instructors in the study request granular, interpretable data on how learners use course materials, complete tasks, and interact with content. CyberSecPro's use of digital platforms can benefit from this by building real-time dashboards, tracking engagement patterns, and using this to personalise learning or flag drop-off points, ultimately improving learner success and course effectiveness.

Bridging the Gap Between Quantitative and Qualitative Evaluation

One of the most important contributions of the Douglas framework is the critique of MOOC platforms relying solely on completion rates or clickstream data. Instead, it proposes integrating qualitative elements such as learner interviews or targeted surveys to understand why learners behave in certain ways. CyberSecPro can use this approach to move beyond superficial metrics and focus on meaningful indicators of impact, especially important for sustainability and recognition.

2.1.4 Biggs' 3P Model

Sebbaq and El Faddouli (2024) applied Bigg's 3P model to explore the quality of massive open online courses (MOOCs). The model depicted educational ecosystems as having foreshadowing, process, and product variables (Gibbs, 2010). Figure 1 showcases the model presented in Sebbag and El Faddouli (2024) to illustrate the approach visually.

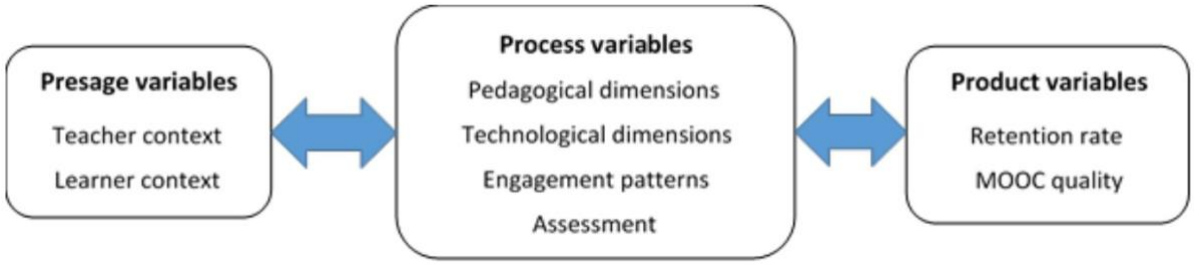

Figure 1: Framework for MOOC Quality Measurement by Sebbag and El Faddouli (2024)

Presage: Traditional measures of presage include factors related to both learner context and teacher context. Regarding the learner context, Sebbaq and El Faddouli (2024) highlight three indicators of quality: learner interaction with activities and content; teacher-learner interaction; and learner-learner interaction and collaboration. Existing research underscores the importance of quality indicators, including the availability of effective activities, tools, approaches, and resources, that assist teachers in improving their teaching experience in relation to the teacher context (Askeroth & Richardson, 2019; Bonk et al., 2018; Ray, 2019). Commonwealth of Learning (2016) affirms that presage variables include the resources and factors that go into the teaching and learning process. These include the learners, instructors, and institutions, as well as, in the case of MOOCs, the platform and the platform provider.

Process: This category pertains to the environment, intricately linked with the presage variables, and includes elements such as instructional design and teaching methodologies. Process variables are broadly divided into four dimensions: pedagogical dimensions, technological dimensions, patterns of engagement, and assessment. These dimensions are described in Table 7.

Product: This category includes metrics such as retention and course completion rates. Sebbaq and El Faddouli (2024), however, note that conventional measures such as retention and completion cannot guarantee quality in MOOCs. They suggest that instructor-oriented factors, course design, and personal factors influence retention and course completion rates, as well as overall MOOC quality.

Table 7: Adapted Bigg's 3P Model Based on Sebbaq and El Faddouli (2024)

Dimension	Examples of Variables	Sub-variables	Description
Presage	Learner quality	Learner-content interaction	Learner interaction with learning activities and content
		Teacher-learner interaction	Learner interaction with teacher
		Learner-learner interaction	Learner interaction with other learners
	Teacher quality	Useful activities, tools, approaches, and resources for teacher development	Availability of these teaching resources
Process	Pedagogical dimension	Pedagogical design	Coherent and integrative course structure
		Pedagogical classification	Classifying MOOCs based on the design features and pedagogical approaches
	Technological dimension	Video features	High-quality videos for active learning
		Gamification	Use of games for learner engagement
		Learning analytics	Data for student improvement
	Patterns of engagement	Persistence, perseverance, interaction, motivation, and communication	Teacher and student working together to foster these qualities for engagement
	Assessment	Formative assessment, summative assessment, and baseline test	Various assessment types are found in MOOCs
Product	Retention and completion rate		Retention and completion indicators need to be complemented with factors related to course design and personal factors

The adapted Bigg's 3P model in Sebbaq and El Faddouli (2024) was not based on a specific discipline, but rather the model was explored from a general perspective.

The linkage/alignment of Sebbaq and El Faddouli (2024) methodology with CyberSecPro

Pedagogical Quality Assurance Framework Tailored to MOOCs

Sebbaq and El Faddouli (2024) propose a micro-level framework for MOOC quality based on Biggs' 3P model (Presage, Process, Product). This model is highly applicable to CyberSecPro, which aims to deliver high-quality, impactful online learning. The framework's comprehensive scope—addressing learner and teacher context, instructional design, technological tools, engagement patterns, and outcomes, gives CyberSecPro a validated structure to assess and improve its course offerings.

Alignment with Learner Diversity and Intent

A core insight from the paper is that learner context matters, including their motivations, goals, background knowledge, and preferred engagement styles. CyberSecPro, targeting a broad European audience with different entry levels into cybersecurity, benefits from this learner-centered design philosophy. The framework encourages personalization and adaptation to diverse learner pathways, a key principle in modern e-learning.

Rich Focus on Instructional Design and Engagement

The authors conducted an extensive literature review to identify proven indicators of MOOC success, providing CyberSecPro with a scientifically robust basis for evaluating and continuously improving their courses.

2.1.5 Stephen and Jones's (2014) Indicators of MOOCs Success from a Student Perspective

Stephens and Jones (2014) explored MOOCs within Library and Information Science (LIS) disciplines. They affirm that MOOCs are a viable means to promote lifelong learning and professional development. Their studies highlight four categories of learners in MOOCS:

- Lurkers: Lurkers benefited from browsing course materials
- Moderately active participants: moderately active participants actively engaged in conversation and some course topics.
- Memorably active participants: This group of learners participate in most topics, completed course assignments, and are active in discussions
- Drop-ins: Drop-ins are engaged in selected topics without ever intending to complete the entire course.

Stephens and Jones (2014) investigated students self-reported success rates and indicators of success in a LIS MOOC program. The indicators are presented in Table 8.

Table 8: Indicators of MOOCs Success Based on Stephen and Jones's (2014)

No	Success indicators and models in MOOCS
1	Students perceive success when they understand core concepts from the course and know they can make direct application of that knowledge
2	Students measured their success based on the amount of interaction they had with their peers
3	Students indicated they did not feel successful due to time constraints
4	Students responded that they felt successful when they participated in writing blogs, received comments on their blogs, and engaged their peers in discussion throughout the course
5	Students enjoyed the variety of viewpoints provided by the course content, instructors, and guest lecturers.
6	Students often talked about how they enjoy collaborating in the community and building professional network.
7	Other indicators include completion of assignments, working towards the certificate, and consuming course readings

The linkage/alignment of Stephen and Jones (2014) methodology with CyberSecPro

Effective Framework for Professional Development
Stephens and Jones explored how MOOCs can effectively serve as professional development platforms, particularly emphasizing knowledge transfer, professional growth, and community building among library and information science (LIS) professionals. CyberSecPro, similarly targeting professional learners in the cybersecurity sector, can use this framework to structure MOOCs as engaging, practical, and professionally beneficial experiences.

Community-Centered Approach (cMOOC Model)
The authors implemented a connectivist MOOC (cMOOC) model, which fosters social learning, networking, and peer collaboration. This aligns strongly with CyberSecPro's need for interactive learning environments, crucial in cybersecurity education, where professional dialogue, shared experiences, and peer-learning significantly enhance understanding of real-world challenges.

Practical Insights for Course Design and Delivery
Stephens and Jones provide concrete insights into MOOC design, including course length, workload balance, module structuring, and assignment flexibility. CyberSecPro can directly apply these insights to optimize its own course offerings, making them more manageable and attractive for busy cybersecurity professionals.

Robust Evaluation Methodology
The use of web-based surveys and content analysis by Stephens and Jones provides CyberSecPro with a proven methodology for systematically gathering learner feedback, measuring course effectiveness, and continually refining course design, essential for meeting quality standards and demonstrating impact in the context of EU-funded initiatives.

Moving Beyond Course Completion
Their study highlights that successful MOOCs shouldn't just focus on completion rates, but rather on meaningful engagement, practical knowledge application, and learner satisfaction. This perspective aligns with CyberSecPro's goal to evaluate professional skills acquisition, learner interaction, and knowledge applicability over mere completion statistics.

Emphasis on Learner Diversity and Accessibility
The authors emphasized accessibility, diversity of viewpoints, and inclusivity in their course design. CyberSecPro similarly serves a diverse European audience, making this emphasis on inclusive learning and flexible, accessible education particularly relevant.

2.1.6 Quality Assurance Methods Assessing Instructional Design and Active Learning Pedagogies in MOOCs

Aloizou (2018) applied the quality standards from Quality Management Higher Education Rubrics to assess a five-week "Innovative and Collaboration Learning with ICT" (CLAT MOOC), which targeted pre-service and in-service teachers interested in incorporating collaboration with technology into their own teaching practices. The standards are presented in Table 9.

Table 9: Rubric for Quality Management in Higher Education Based on Aloizou (2018)

Standards	Indicators or descriptions
Course overview and introduction	Instructions make clear how to get started and where to find various course components.
	Learners are introduced to the purpose and structure of the course.
	Etiquette expectations for online discussions, email, and other forms of communication are clearly stated.
	Course and institutional policies with which the learner is expected to comply are clearly stated
	Minimum technology requirements are clearly stated and instructions for use provided
	Prerequisite knowledge in the discipline and any required competencies are clearly stated
	Minimum technical skills expected of the learner are clearly stated
	The self-introduction by the instructor is appropriate and is available online
	Learners are asked to introduce themselves
Learning objectives	The course learning objectives describe outcomes that are measurable
	The module/unit learning objectives or competencies describe outcomes that are measurable and consistent with the course-level objectives or competencies
	All learning objectives or competencies are stated clearly and written from the learner's perspective
	The relationship between learning objectives or competencies and course activities is clearly stated
	The learning objectives or competencies are suited to the level of the course

Assessment and measurement	The assessments measure the stated learning objectives or competencies
	The course grading policy is stated clearly
	Specific and descriptive criteria are provided for the evaluation of learners' work and are tied to the course grading policy
	The assessment instruments selected are sequenced, varied, and suited to the learner work being assessed
	The course provides learners with multiple opportunities to track learning progress
Instructional materials	The instructional materials contribute to the achievement of the stated course and module/unit learning objectives or competencies
	Both the purpose of instructional materials and how the materials are to be used for learning activities are clearly explained
	All instructional materials used in the course are appropriately cited
	The instructional materials are current
	Various instructional materials are used in the course
	The distinction between required and optional materials is clearly explained
Course activities and learner interaction	The learning activities promote the achievement of the stated leaning objectives or competencies
	Learning activities provide opportunities for interaction that support active learning
	The instructor's plan for classroom response time and feedback on assignments is clearly stated
	The requirements for learner interaction are clearly stated
Course technology	The tools used in the course support the learning objectives and competencies
	Course tools promote learner engagement and active learning
	Technologies required in the course are readily obtainable
	The course technologies are current

	Links are provided to privacy policies for all external tools required in the course
Learner support	The course instructions articulate or link to a clear description of the technical support offered and how to obtain it.
	Course instructions articulate or link to the institution's accessibility policies and services
	Course instructions articulate or link to an explanation of how the institution's academic support services and resources can help learners succeed in the course and how learners can obtain them
Accessibility and usability	Course navigation facilitates ease of use
	Information is provided about the accessibility of all technologies required in the course
	The course provides alternative means of access to course materials in formats that meet the needs of diverse learners
	The course design facilitates readability
	Course multimedia facilitates ease of use

According to Aloizou (2018), participants used a five-point Likert scale to rate each indicator, where 1 represented 'strongly disagree' and 5 represented 'strongly agree'; these ratings were then used to determine the overall evaluation of the MOOC.

The linkage/alignment of Aloizou (2018) methodology with CyberSecPro

Focus on Instructional Design and Active Learning Pedagogies

Aloizou's study specifically evaluates how quality assurance (QA) methods assess instructional design in MOOCs, especially those using active learning strategies such as collaborative learning and gamification. This aligns directly with CyberSecPro's mission to create cybersecurity MOOCs that are not only content-rich but also pedagogically sound and engaging. Active learning is crucial in cybersecurity training, where hands-on and problem-based activities are essential.

Use of Real-World Case Study (CLAT MOOC)

The study employs the CLAT MOOC as a practical testbed, analyzing its collaborative and gamified design using selected QA tools. This hands-on methodology is highly relevant for CyberSecPro, which also aims to develop MOOCs with applied, skill-focused learning. The framework demonstrates how real courses can be evaluated meaningfully using both qualitative and quantitative inputs—something CyberSecPro can replicate with its pilot courses.

Responsive, Modular Evaluation Approach

Aloizou emphasizes that no single QA tool is fully sufficient, highlighting the need for modular, adaptive evaluation tools that reflect specific pedagogical goals. This is key for CyberSecPro, where different modules may require distinct evaluation metrics (e.g., for labs, simulations, quizzes, or group projects).

2.1.7 Tzeng et al.'s (2022) MOOC Evaluation System Based Student Sentiment Survey

Tzeng et al. (2022) adopted five categories of student sentiment surveys to evaluate 17 MOOCs at the National Tsing Hua University. The following MOOCs were assessed:

- Introduction to IoT (Internet of Things)
- Introduction to Calculus
- Introduction to Programming in Python
- Financial Decision Analysis
- Systems Neuroscience
- Ecosystem and Global Changes
- Common Good in Social Design
- Introduction to Data Structure
- Introduction to Calculus

- AP-General Physics
- AP-General Chemistry
- AP-Introduction to Life Sciences
- AP-Principles of Economics
- AP-Introduction to Computer Science
- AP-Introduction to Programming in Python
- AP-Introduction to Computer Programming

Students in these MOOCs were expected to spend three hours each week watching online videos and completing practice exercises. They were also expected to discuss the course content with their peers. For Introduction to IoT, students were also required to conduct experiments in some offline laboratory sessions. Tzeng et al. (2022) used a five-point Likert scale to evaluate the answers provided by students, where 1 represented 'strongly disagree' and 5 represented 'strongly agree'. The ratings were then used to determine the overall evaluation of the MOOC.

Table 10: MOOC Evaluation System Based on Tzeng et al. (2022)

Dimension	Indicator or description
Workload	It takes a lot of time to watch the videos for this course
	I think this course is quite difficult
	I can keep up with the subsequent courses without spending much time reviewing
Need fulfilment	The course material is consistent with what I expect to learn
	The course material is not what I currently need to learn.
	This course will be helpful for my future courses and research
	This course is helpful for my future job search
	This course is related to my major
Intelligibility	The teacher’s style helps me easily understand the content
	The teacher can explain the key points and clarify confusing points.
	The teacher’s method is too disorganized for me to keep up
	The teacher is unclear, and I have difficulty understanding.
	The teacher’s methods make me feel that this course is an efficient way to learn

Style approval	The teacher's style makes me eager to learn.
	The way the teacher speaks makes me feel a little hesitant.
	The teacher's tone does not make me feel irritated
	The teacher's rhythm puts me at ease
	The teacher's methods make me feel pressured.
Student engagement	I watched the course videos at least once before the end of the course
	I review the exercises by myself offline
	I will find related videos about unfamiliar concepts
	I will re-watch videos to review unfamiliar concepts

The linkage/alignment of Tzeng et al. (2022) methodology with CyberSecPro

Data-Driven MOOC Evaluation Using AI and Deep Learning

Tzeng et al. introduce an innovative MOOC evaluation system that predicts student satisfaction using deep learning models based on learner behavior data (e.g., video interactions, quiz activity). This is highly applicable to CyberSecPro, which delivers MOOCs to large, diverse audiences where traditional surveys may yield low response rates. Using AI to monitor engagement and satisfaction enables CyberSecPro to perform continuous, automated, and scalable course evaluation.

Advanced Learning Analytics and Behavior Modeling

Tzeng et al. extract and analyze detailed behavioral data—such as playback speed, number of replays, and time spent per exercise—which provides CyberSecPro with a roadmap for applying granular learning analytics. These insights are especially valuable in cybersecurity education, where engagement with technical content (e.g., coding or simulations) is critical.

Scalable and Automated Evaluation for Large-Scale MOOCs

CyberSecPro, as a Europe-wide initiative, must operate at scale. Tzeng's framework shows how AI can replace or augment manual feedback mechanisms, saving time and resources while providing consistent and timely insights. This supports CyberSecPro's goals of efficiency and quality assurance across its course offerings.

Personalized Feedback and Course Adjustment

The system proposed by Tzeng et al. allows for predictive personalization, alerting instructors to learners who may struggle, and prompting adjustments in pacing, difficulty, or support. CyberSecPro can adopt this to create more adaptive and responsive cybersecurity training pathways, improving learner outcomes and satisfaction.

2.1.8 Duan and Wu's (2023) Student Self-Assessment Paradigm in MOOCs

To analyse the self-assessment of Chinese students in MOOCs, Duan and Wu (2023) implemented and customized the Seven Pillars of Assessment. Student self-assessment is a comprehensive assessment in which students try to find the changes in their deep and implicit learning. The main contents of the Seven Pillars Theory are described in seven basic questions in the assessment area: "Why Assess", "How to Assess", "What to Assess", "When to Assess", "Who Assesses", "How Well", and "Whither." Each of these questions are based on distinct principal factors outlined in Table 11.

Table 11: The Principal Factors of Student Self-Assessment Based on Duan and Wu (2023)

Dimension	Factor	Meaning
Why Assess	Motivation for assessment	To continuously optimize student MOOC-based learning
	Assessment objective	Effective MOOC learning
How to Assess	Assessment method	Qualitative and quantitative methods. For example, self-assessment rubrics, self-assessment scripts, reflective logging and so on
What to Assess	Assessment technology	Network evaluation techniques like computer adaptive testing and e-assessment
	The gaining of knowledge and skills	Knowledge, skills, and cognitive processes
When to Assess	Continuity of self-assessment process	Student self-assessment runs through the whole process of learning
Who Assesses	Assessor	The students themselves are given priority, and teachers and peers are supplemented
How Well	Reliability of assessment	To ensure the accuracy and realism of student self-assessment
Whither	Appreciation of self-assessment	Student self-assessment becomes the basis of MOOC evaluation

The above student self-assessment in MOOCs was not applied to any particular academic discipline in Duan and Wu (2023), suggesting the model can be applied to various MOOC settings involving student self-assessment. The dimensions and descriptors in Table 11 serve as a reference for designing questions aimed at assessing the quality of MOOCs.

The linkage/alignment of Duan and Wu (2023) methodology with CyberSecPro

Promotes Student-Centered Learning Through Self-Assessment

Duan and Wu propose an integrated student self-assessment paradigm specifically for MOOCs. This model emphasizes shifting from teacher-dominated evaluation to learner-centered, formative self-assessment, which perfectly aligns with CyberSecPro's goal of empowering learners in cybersecurity education to take greater ownership of their learning progress.

Framework for Scalable, Lifelong Learning Competencies

Self-assessment is framed as a core competency for lifelong learning, a key pillar in EU digital and green transitions. CyberSecPro's microcredentials aim to upskill professionals who must adapt continuously. The Duan and Wu framework supports this by encouraging learners to monitor, evaluate, and reflect on their own skill development—particularly relevant in a rapidly evolving field like cybersecurity.

Multi-Level, Structured Model for Implementation

The authors build their model using Interpretive Structural Modeling (ISM) and MICMAC analysis, identifying nine interrelated factors influencing student self-assessment. These are categorized into surface, middle, and deep factors, offering CyberSecPro a systematic blueprint for embedding self-assessment at various levels—ranging from tool design to learner motivation and skills.

Supports Quality Assurance and Assessment Diversity

The model positions self-assessment as a valid, reliable, and formative assessment method, especially crucial in asynchronous and self-paced MOOCs like those in CyberSecPro. It enables the integration of qualitative (e.g., reflection scripts) and quantitative (e.g., rubrics) tools, enhancing assessment diversity and quality assurance.

Encourages Reflective and Metacognitive Skills

The framework advances metacognitive development, helping learners in CyberSecPro become more reflective, adaptive, and strategic. In cybersecurity, this supports not only technical proficiency but also critical thinking and problem-solving, which are essential for real-world application.

2.1.9 Evaluation Requirements Based on ENQA Considerations

Ferreira et al. (2022) proposes a system of requirements and indicators for evaluating MOOCs based on the European Association for Quality Assurance in Higher Education (ENQA) considerations. The authors implemented the Delphi method, which involved successive rounds of application based on

expert judgment, to establish the evaluation system. The requirements and indicators are detailed in Table 12.

Table 12: Considerations for MOOC Evaluation Based on Ferreira et al. (2022)

Dimension	Indicator or description
Policy for quality assurance	The MOOC foresees an evaluation system for improvement that includes satisfaction surveys of stakeholders, especially learners (quality assurance of the course itself)
Design and approval of programs	People involved in designing/developing/evaluating MOOC programs have expertise in academic and technical aspects
	Learner needs (including special educational needs if applicable) are considered when developing the learning model and the curricula design
Student-centred learning, teaching, and assessment	Teaching methodologies and learning activities are chosen with the aim of achieving learning outcomes
	Learning materials fit the pedagogical model and facilitate student learning
	E-assessment methods are fit for purpose, allowing students to demonstrate the extent to which the intended learning outcomes have been achieved
	Learners are aware of plagiarism rules
	Learning materials are relevant and are reviewed and updated periodically
	Learners are clearly informed about the e-assessment
	The VLE provides the appropriate methods and tools that support effectively the achievement of the learning outcomes
	The MOOC fosters interactions between learners
Student admission, progression, recognition, and certification	Learners are informed about the workload and pedagogical model of the MOOC program

	Learners/prospective learners are informed about requirements concerning equipment, MOOC and digital skills, pre-knowledge and prerequisite subjects, and attendance
Teaching staff	Technological and pedagogical support services for educators are adequate, accessible, and timely
	There are coordination mechanisms for the educational staff involved, if applicable
Learning resources and student support	The technical infrastructure ensures the accessibility of the MOOC program by learners with special educational needs
	The MOOCs ensure the electronic security measures that uphold quality standards and the validity and integrity of information
Information management	The MOOC considers ethical norms and government policy regarding data protection and the privacy of learners
	Collected data is used to evaluate the MOOCs program (e.g. comparative analysis of course design)
Public information	The MOOC publishes reliable, complete, and up to date information on itself (i.e. recognition of qualifications, learning objectives, credits, requirements, assessment methods, timelines, dates relevant for the program
	Technical requirements to enable the full and effective use of the system are clearly identified and published
Ongoing monitoring and periodic review of programs	ICT and pedagogy developments are analysed and implemented when appropriate

The above MOOC evaluation model in Ferreira at al. (2022) was not applied to any particular discipline, suggesting the model can serve as a general set of points to consider when evaluating MOOCs.

The linkage/alignment of Ferreira's (2022) methodology with CyberSecPro

EU-Aligned Quality Assurance Framework

Ferreira et al. present a robust framework for evaluating MOOCs based on ENQA (European Association for Quality Assurance in Higher Education) standards. This directly aligns with CyberSecPro's EU-funded mandate to ensure high pedagogical, institutional, and technological quality in its training programs. The indicators were validated using the Delphi method, ensuring consensus from international MOOC experts.

Applicable to Diverse Learners and Lifelong Learning

The study emphasizes relevance, feasibility, and comparability of each quality indicator across different learner profiles, including adult learners and professionals. This supports CyberSecPro's aim to serve a diverse audience across the EU with accessible, transferable, and relevant cybersecurity training.

Supports Institutional Validation and Recognition

The checklist developed can help CyberSecPro partners internally validate MOOCs and facilitate their recognition by higher education institutions, employers, and QA agencies. This supports the project's goals for trustworthy microcredentials and mainstream academic recognition.

2.1.10 Open VM MOOC Framework

Poce et al. (2019) present a case study focusing on quality assurance framework for a MOOC created in the Erasmus+ Virtual Mobility Project. Virtual Mobility in this context refers to ICT supported activities organized at higher education level, that facilitates international, collaborative experiences in a context of teaching and learning. The three main macro-indicators identified for MOOC evaluation are based on the ACHIEVE model. They include quality, appropriateness, and technical aspects.

Each macro-indicator was operationalized through sub-indicators (Table 12). By combining the answers on different sub-indicators, it is possible to provide a general overall evaluation of the OER (0 = not usable; 1 = limited; 2 = good; 3 = superior). For instance, a resource may be deemed inadequate if it is not current, peer-reviewed, or accessible to individuals with disabilities. On the other hand, a resource is considered superior if it covers one of the MOOC's topics, if it is updated and its contents are clearly organized and accessible to different kinds of targets. The table was mainly inspired by a separate rubric for the evaluation of OERs created by ACHIEVE.org, a non-profit education organization created in 1996 by a bipartisan group of governors and business leaders, fully recognized by international companies and institutions.

Table 13: OER Rubrics Adapted from the ACHIEVE Model Based on Poce et al. (2019)

Indicator	Sub-dimension	Descriptive questions
Quality	Creator knowledge	Who is the creator and what kind of expertise and experience do they have?
	Creator authenticity	Are you reasonably certain that it is the work of the person claiming to be the author?
	Creator bias	What is the intended purpose? (educate/inform, sell something, entertain, change minds/behaviour, propaganda/hate speech)
	Organization affiliation	What is the hosting organization and what kind of reputation do they have?)
	Organization quality control	Does the hosting organization conduct any sort of quality control?
	Peer reviewed	Has it been through peer review?
	Material(s) currency	How recent or up to date is its content?
	Type of assessment	True/False; multiple choices; filling in the blanks; matching; open-ended
Appropriateness	Clarity of structure and content	(Descriptive questions not available)
	8 badges topics	Intercultural skills, Collaborative learning, Autonomy-driven learning, Networked learning, Media and digital learning, Active Self-regulated learning, Open mindedness, VM knowledge
	Difficulty level	**Beginner**: a video that offers a general definition of the skill OR a resource written in simple language that does so. **Intermediate**: resources that are written in a clear and concise manner and which connect the skills to potential applications, or a video that demonstrates how the skill can be applied in specific circumstances. **Advanced**: resource that is composed of intricate or academic language and addresses real-world, undefined issues OR video that illustrates the

		interconnections and complexity of the skill in relation to other skills, ethical considerations, and so forth
Technical aspects	Licensing status	What is its copyright and licensing status, and how does that impact what you can do with it?
	Human accessibility	Is it accessible to people with disabilities?
	Remix or edit	If you want to remix it, is the source file available, and in a format that you can edit?
	Technical accessibility	Is it accessible to people using different devices (multichannel)?
	Technical Quality	In terms of graphics, sound, text layout)
	Numbers of items in the e-assessment	(Descriptive questions not available)

Scoring rubric: (0 = not usable; 1 = limited; 2 = good; 3= superior)

The above evaluation rubric was applied to MOOCs that promote virtual mobility and open education, as demonstrated in Poce et al. (2019).

The linkage/alignment of Poce et al. (2019) methodology with CyberSecPro

Structured Quality Assurance for MOOCs and OERs

Poce et al. (2019) introduce a practical and multi-dimensional MOOC Quality Assurance Framework, applied in the context of the Erasmus+ Open Virtual Mobility project. This model is directly relevant to CyberSecPro's goal of developing high-quality cybersecurity MOOCs, as it focuses on evaluating both full courses and the Open Educational Resources (OERs) embedded within them.

Use of a Validated Rubric for OERs

The framework includes a detailed rubric that assesses OERs based on three macro-indicators:

- Quality (e.g., expertise of creator, peer-review, bias),
- Appropriateness (e.g., relevance, difficulty level, alignment with MOOC content),
- Technical aspects (e.g., accessibility, licensing, editability, and technical quality).

Alignment with Iterative, Design-Based Research (DBR) Approach

The study follows the Design-Based Research (DBR) model for continuous improvement, using internal peer review, external expert review, learner feedback, and learning analytics. This iterative model fits CyberSecPro's needs to develop, test, and refine its MOOC content through pilot testing and feedback loops across multiple partners and platforms.

Focus on Digital and Pedagogical Innovation

The OpenVM MOOC structure (24 subMOOCs across 8 skill areas and 3 difficulty levels) showcases modular, flexible, and skill-oriented course design, with embedded e-assessment and badge-based certification. These features align with CyberSecPro's vision of microcredential pathways that support upskilling, certification, and lifelong learning in cybersecurity.

2.1.11 Sabjan et al.'s (2021) MOOC Quality Design Criteria in Programming and Non-Programming Courses

Sabjan et al. (2021) investigates the quality design criteria for designing MOOCs from the perspective of programming and non-programming students. The MOOC categorized under the Programming subject is Intro to Object-Oriented Programming. The MOOCs categorized under the non-programming subjects are Islamic Banking Management, Export Management, International Business, Accounting System Analysis and Design, Technology Planning and Management in Education, Islamic Bank Operation, Human Lifespan Development, Foundations of Banking, and Fundamentals of Entrepreneurship. The findings from the study are described in Table 13.

Table 14: MOOC Quality Design Criteria Based on Sabjan et al. (2021)

Student category	Values	Description
Programming students	Instructional design	Courses with clear objectives and structured progress timelines
		Exercises that help understand syntax and error patterns
	Video content	Synchronization between video, notes, and programming examples
		Rich video content with technical details (e.g. IDE usage)
	Technical tools	Need help systems focused on user errors
		Prefer email notifications and live programming examples
	E-assessment	Strong emphasis on getting feedback and correct answers
		Need continuous feedback to track progress and reduce programming errors
	Culture	Favour neutral, English-based content
		Require universally understandable examples, minimizing cultural confusion
Non-programming students	Instructional design	Want self-organized learning through clear course guidelines
		Emphasize support for self-coordination
	Video content	Prefer short video clips (≤ 20 minutes)
		Appreciate references and factual backing in videos for further exploration
	Technical tool	Like the ability to download videos
		Prefer collaborative tools and discussion forums
	E-assessment	Prefer hints and diverse question types during assessments
		Need feedback and explanation to understand theoretical content

	Culture	Content that reflects cultural diversity, e.g. video recognizing varied backgrounds

The linkage/alignment of Sabjan et al. (2021) methodology with CyberSecPro

Focus on Tailored MOOC Quality Design Criteria

Sabjan et al. (2021) identify and empirically validate MOOC design quality criteria by comparing the needs of programming vs. non-programming students. This is directly relevant to CyberSecPro, which develops cybersecurity training, a technical domain similar to programming. Their framework helps ensure that the specific needs of technical learners are addressed through tailored instructional, technical, and assessment design strategies.

Multi-Dimensional Evaluation Framework

- The study introduces a structured evaluation framework based on three core dimensions:
- Instructional Design (lecture organization, cultural considerations),
- Technical Features (user interface, video content, learning tools, analytics),
- E-Assessment (feedback, hint provision, question formats).

This framework aligned with CyberSecPro approach for evaluation that designed to be multi-modular which can be easily adjusted to each type of the learning activity.

Validated Insights into Diverse Learner Needs

The study shows that different student groups (technical vs. non-technical) prioritize different features in MOOCs. CyberSecPro can use this to design learner-centered pathways for beginners and advanced learners in cybersecurity, improving personalization and inclusivity.

Evidence-Based Recommendations for MOOC Developers

Sabjan et al. provide actionable design insights—like using an integrated development environment (IDE) for programming courses, or offering structured feedback and learning analytics, which CyberSecPro can adopt to enhance its instructional effectiveness and student engagement.

2.1.12 Shah et al.'s (2023) Framework for Formative Evaluation of MOOC Pedagogy

One way to ensure the quality of MOOCs is through systematic evaluation of its pedagogy with the goal to improve over time. However, most existing MOOC's quality evaluation methods do not account for the increasing significance of learner-centric pedagogy towards providing a richer learning experience.

Shah et al. (2023) presents a MOOC Evaluation Framework (MEF), designed with a strong pedagogical basis underpinned by theory, MOOC design practices, and learner-centric pedagogy.

Table 15: List of All Dimensions and Criteria in the MEF by Shah et al. (2023)

Dimension	Criteria or Indicator
Course structure and expectations	Course framework and content
	Prerequisites for the course
	Comprehending course components
	Guidelines for learner interactions with content and peers
	Exams and grading policy
	Communication with course team
Video content	Video content appropriateness
	Video chunk length
	Presence of in-video activities
	Purpose of in-video activities
	Positioning and time span of in-video activities
	Feedback on in-video activity and its nature
	Video content presentation
Learning resources	Offering of supplementary learning resources
	Addressing diverse learner needs and interests
	Ensuring learner engagement with resources
Discussion forum	Opportunities and goals of interaction activities on the forum
	Design of peer interaction activities
	Moderator support
	Feedback on forum

	Clear communication
	Integration of technology tools
Synchronous interactions	Opportunities for synchronous interactions
	Purpose of synchronous interactions
	Update on upcoming interaction
	Effective conduct of interaction
	Ease of technology for participation
	Availability of interaction videos
Assessment (formative and summative)	Presence of formative assessment activities
	Frequency of assessment opportunities
	Format of assessment activities
	Pedagogical role of assessment activities
	Feedback on assessment
	Grading of assessment activities
	Grading strategies
Content alignment and integrity	Constructive alignment
	Alignment of technology and pedagogy
	Academic integrity
Learner connection practices	Prompt communication
	Motivating learners
	Support for learner agency
	Community building
	Understanding learner difficulties
	Learner feedback

Each indicator is rated on a 4-point scale (missing, inadequate, adequate, or proficient) ranging from 0 to 3, demonstrating the level of performance. An overall judgement can be made on the extent to which

a benchmark indicator is achieved. Shah et al. (2023) applied the MEF to evaluate MOOCs across disciplines including Computer Science, Instructional Design, Chemistry, Management, Analytics, and Maths, suggesting its broader applicability.

The linkage/alignment of Shah et al. (2023) methodology with CyberSecPro

Learner-Centric Pedagogical Evaluation

Shah et al. (2023) propose a MOOC Evaluation Framework (MEF) specifically designed to assess the integration of learner-centric pedagogy, including active learning, peer interaction, feedback, and instructor presence. This is relevant to CyberSecPro since it is committed to promoting meaningful learner engagement and autonomy in cybersecurity training, which are key to developing real-world professional competencies.

Comprehensive Dimensions for Course Evaluation

The MEF evaluates MOOCs across eight structured dimensions, such as course structure, video content, assessment design, discussion forums, and learner connection practices. This is relevant to CyberSecPro as it delivers modular, stackable microcredentials where a clear, consistent structure and pedagogical coherence are essential to ensure high-quality learning experiences across all modules and partner institutions.

Emphasis on Formative Evaluation and Course Improvement

The framework is built for formative evaluation, enabling course creators to assess and enhance their MOOC design during development, using detailed indicators and performance benchmarks. This is relevant to CyberSecPro as it emphasizes iterative improvement and responsiveness to learner feedback, ensuring that courses remain dynamic, effective, and adaptable across diverse learner contexts.

2.1.13 Stracke et al.'s (2018) European MOOC Quality Reference Framework

Stracke et al. (2018) address the open issue of integration of quality approaches and mechanisms into the design of MOOCs by developing the European MOOC Quality Reference Framework (QRF). The MOOC QRF offers a generic, organization-wide system to support higher education institutions and external stakeholders in the design, development, monitoring, evaluation and continuous improvement of MOOCs, alongside their quality management practices. Rooted in the first international quality standard, ISO/IEC 40180, the QRF has been submitted to both the European and international standardization committees (CEN TC 353 and ISO/IEC JTC1 SC36) for approval as the first dedicated quality standard for MOOCs. Table 15 outlines the structure and quality dimensions of the QRF, while Figure 2 illustrates its five implementation phases.

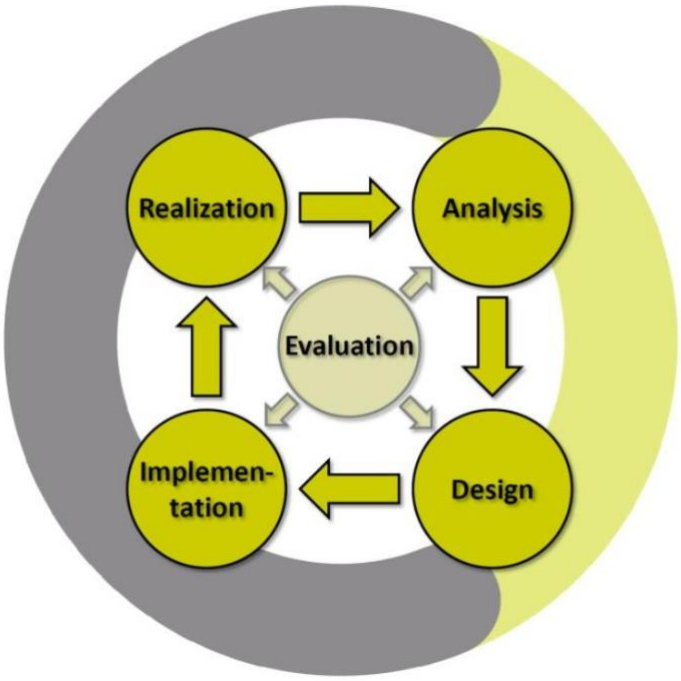

Figure 2: The Phases of the QRF by Stracke et al. (2018)

Table 16: Overview of the MOOC QRF Based on Stracke et al. (2018)

Dimension	Components	Description	Purpose
Phases	Analysis	Identifying and describing requirements, demands, and constraints	Provides a step-by-step lifecycle for MOOC development; supports iterative and cyclical quality improvement
	Design	Conceptualizing and design of the MOOC	
	Implementation	Implementing a MOOC draft and finalizing it through testing	
	Realization	Realizing and performing the MOOC, including support and assessment	
	Evaluation	Defining, running and analysing the evaluation and improving the MOOC	
Perspectives	Pedagogical	Learning, design, and teaching strategies	Ensures that all MOOC development aspects are addressed across all phases
	Technological	Platform functionality and tool usability	
	Strategic	Institutional alignment and sustainability	
Roles	Designer	Content creators, tech, and support designers	Assigns responsibilities and fosters collaboration among stakeholders involved in the MOOC industry
	Facilitator	Tutors, moderators, and support staff	
	Provider	Institutions, platform owners, and decision-makers	
Benefits	Practical use of the QRF	Adaptable to diverse MOOC contexts	
		Supports continuous improvement of MOOCs	

The linkage/alignment of Stracke et al. (2018) methodology with CyberSecPro

Provision of a Comprehensive MOOC Quality Reference Framework (QRF)

Stracke et al. (2018) present a Quality Reference Framework (QRF) developed by the MOOQ initiative to support the design, delivery, and evaluation of MOOCs. This is relevant to CyberSecPro since it is a project focused on developing high-quality, standardized cybersecurity microcredentials and needs a structured framework to ensure consistent pedagogical and organizational quality across its consortium partners.

Alignment with EU Policy Priorities on Open Education and Quality Assurance

The QRF is grounded in the European Commission's agenda on Opening Up Education and aims to respond to the increasing demand for flexible, quality-assured learning in higher education. This is relevant to CyberSecPro as it is framed by the same EU strategic priorities and must demonstrate alignment with European standards for online education quality and openness.

Three-Dimensional Approach to MOOC Quality

The framework introduces a three-dimensional structure: phases (e.g. design, implementation, evaluation), perspectives (pedagogical, technological, strategic), and roles (designer, facilitator, provider). This is relevant to CyberSecPro as it operates through a multi-actor model across partner institutions and needs clear guidance on how to distribute quality responsibilities throughout the lifecycle of the evaluation.

Support for Continuous Improvement and Standardization

The QRF emphasizes formative evaluation and continuous improvement cycles, and it is being considered for standardization at the European (CEN) and international (ISO) levels. This is relevant to CyberSecPro as it aims to build credible and transferable cybersecurity microcredentials that must withstand external scrutiny and align with formal standards.

Evidence-Based Development from Pan-European Stakeholders

The framework is developed using mixed methods research, incorporating insights from MOOC learners, designers, and facilitators through surveys and interviews. This is relevant to CyberSecPro since it is a collaborative, multi-country project that also relies on stakeholder engagement and research-informed design to address user needs and improve learning effectiveness.

2.1.14 Yilmaz et al.'s (2017) Online Learning Environment Evaluation Form

Yilmaz et al. (2017) developed an Online Learning Environment Form (OLEF) to evaluate six MOOCs selected from the Udemy platform. The evaluated MOOCs included: 'First Impression,' 'Confidence,' 'Storytelling,' 'Time Management,' 'Java,' and 'Android.' The OLEF is structured around eight categories, each containing specific items. Below is a summary table outlining the categories, number of items, description, and sample evaluation in percentage.

Table 17: Overview of the OLEF Based on Yilmaz et al. (2017)

Category	No. of items	Description	Score (%)
Communicate high expectations	4	Assesses whether the course clearly defines expectations, objectives, and student responsibility.	100%
Ease of use	7	Evaluates platform usability, clarity of navigation, downloadability of materials, and accessibility.	87.71%
Emphasizing time on task	2	Checks if the course supports time management through tools like syllabi and announcement boards.	100%
Encourage active listening	3	Measures the use of varied assessments, hands-on learning, and logical course flow.	61%
Feedback	4	Evaluates whether learners and instructors receive timely, useful feedback on progress.	75%
Respect diverse talents and ways of learning	5	Assesses responsiveness to different learning styles, prior knowledge, and personalization options.	43%
Student-student interaction	6	Reviews tools and opportunities for peer communication and collaboration.	67%
Student-faculty interaction	2	Evaluates opportunities for meaningful interaction with instructors.	91.6%

The "No. of Items" column refers to the number of evaluation statements or questions that were used to assess each category in the OLEF, showing how thorough or multidimensional the evaluation was for that aspect of the learning environment. Yilmaz et al. (2017) indicate that the quality dimension outlined in Table 16 served as a reference for designing evaluation surveys, which participants completed and scored to assess the overall quality of the selected MOOCs.

The linkage/alignment of Yilmaz et al. (2017) methodology with CyberSecPro

Use of Instructional Design Principles for MOOC Evaluation

Yılmaz et al. evaluate MOOCs using a custom-built framework derived from Chickering and Gamson's Seven Principles for Good Practice, a foundational model in instructional design. This is relevant to CyberSecPro as it is committed to developing high-quality, pedagogically sound cybersecurity MOOCs that must align with recognized principles of effective teaching and learning, especially to ensure active engagement in self-paced, open learning formats.

Identification of Weaknesses in Active Learning and Learner Diversity

The study found that MOOCs often fall short in supporting active learning and diverse learning styles, two areas critical for learner engagement and inclusivity. This is relevant to CyberSecPro as it aims to serve a diverse group of learners across Europe, many of whom have different learning needs, prior experience levels, and professional backgrounds, and therefore require personalized and flexible pedagogical strategies.

Focus on Learner Interaction and Communication Channels

The evaluation emphasized the importance of student-faculty and student-student interaction, with findings showing limited support for peer collaboration and instructor feedback. This is relevant to CyberSecPro as it integrates collaborative learning tools and instructor presence as key features of its MOOC strategy to foster a stronger sense of community and support, which is especially important in cybersecurity training environments.

Attention to Platform Usability and Accessibility

The study assesses MOOC platforms for ease of use and accessibility, particularly for learners with physical disabilities. This is relevant to CyberSecPro as it is committed to making its learning platforms inclusive and user-friendly, ensuring that all participants, including those with accessibility needs, can effectively engage with course materials.

Application of Evaluation Tools Based on Contextual Adaptation

Yılmaz et al. developed a tailored evaluation instrument adapted to the Turkish context and the Udemy platform, showing the value of localizing evaluation tools for MOOC quality analysis. This is relevant to CyberSecPro as it operates across a range of national and institutional contexts, where flexibility in quality assurance tools is necessary to respect cultural and institutional diversity while maintaining common standards.

2.1.15 BIBLIO MOOC Evaluation Form

The BIBLIO project developed a digital MOOC designed to help learners to develop digital and transversal skills essential for library professionals in the digital era. According to Gatomati et al. (2021), the MOOC incorporates videos, presentations and reading materials, and fosters tutor-learner collaboration and peer learning through forums and chats. At the end of each unit, participants can self-assess their progress, and the overall quality of the MOOC can be evaluated using an online evaluation form (Table 18). While this MOOC primarily targets librarians and those working in the field, it is also suitable for anyone interested in understanding the evolution of the information sector and the potential of digitalization in libraries. The MOOC offered 26 modules covering transferrable and digital skills for library professionals (Table 17). 295 learners from Bulgaria, Greece, Italy, and Latvia completed the evaluation form and their responses are outlined in Table 19, to depict how the evaluation criteria can be used in other contexts.

Table 18: MOOC Modules by Gatomati et al. (2021)

Modules	
1	Introduction to digitization
2	Spotting opportunities
3	Interacting through digital technologies (online meetings)
4	Digital tools and digital content development
5	Managing digital identity
6	Protecting data and content
7	User support (Identifying needs and responses)
8	Competency management
9	Strategic thinking (Business plan development)
10	Identifying and evaluating fake data, information, and digital content
11	Collaboration and sharing through digital technologies
12	Copyright legislation
13	Basic principles of data safety and security
14	Protecting personal data and privacy
15	Problem/ crisis management

16	Design thinking
17	Valuing ideas
18	Managing data, information, and digital content
19	Marketing and promotion
20	Sales development
21	Mobilizing resources
22	Change management (Change support)
23	Project management
24	Time management
25	Advocacy
26	Risk management

Table 19: BIBLIO MOOC Evaluation Criteria Based on Gatomati et al. (2021)

Evaluation area	Description	Sample participant feedback
Ease of use	Ease of use of the platform	82% reported no problems using the platform
Technical support need	Whether users needed technical assistance	72% did not need assistance
Functionality of features	All platform functions worked as expected	68% confirmed proper functioning
Platform stability and design	Any platform malfunctions or design flaws	81% reported no issues
Learning curve	Whether participants needed time to learn the platform	Platform was intuitive; no learning curve reported
User confidence	Confidence while navigating	83% felt confident
Information clarity	Information was easy to find	80% agreed

Navigation vs. content clarity	Whether users could distinguish between content and navigation	64% could distinguish easily
Visual appeal	Friendliness and attractiveness of the platform	78% positive responses
Aesthetic design	Overall look and feel	67% rated as aesthetically pleasing
Buttons and labels	Clarity of navigation tools	80% found them clear
Readability	Ease and comfort of reading content	Vast majority found content readable
Security and accessibility	Safe system and accessible for different users	88% positive feedback
Icon clarity	Were icons understandable	95% found icons clear
Tool usability	How well the tools functioned	50% gave high usability ratings
Forms and tools	Usefulness of integrated forms/tools	Mixed feedback; 39 positive responses
Self-paced learning	Time flexibility within the platform	98% said they had enough time
Support for the learning process	Whether the platform facilitated meaningful learning	89% said yes
Presentation quality	Clarity and consistency of slides and presentations	Some criticism: repeated content, unclear slides
Assessment design	Clarity, structure, and language of assessments	Criticism for vagueness and language issues
Communication tools	Forum responsiveness, suggestions for chats and workshops	Suggestions for chatroom integration
Module graphics	Graphics reflecting content themes	Highly rated, matched content well
Overall platform maturity	Perception of platform readiness and usability	Described as mature, user-friendly, and effective

The linkage/alignment of BIBLIO framework with CyberSecPro

Modular Curriculum Mapped to EU Competence Frameworks

The BIBLIO MOOC curriculum is structured into modular, competency-based units aligned with EU frameworks such as DigComp, EntreComp, and the European e-Competence Framework. This is relevant to CyberSecPro as it is also committed to developing learning modules aligned with European qualification frameworks (e.g., e-CF, European Cybersecurity Skills Framework), ensuring both recognition and portability of learning outcomes.

Blended Learning Pathway with Specialization and Work-Based Phases

The BIBLIO training pathway includes a MOOC phase, followed by a specialization course and work-based learning (WBL). This is relevant to CyberSecPro as it incorporates a blended learning model that extends beyond content delivery into applied, experiential learning phases—essential for practical cybersecurity skill development.

User-Centered Design and Platform Usability Evaluation

BIBLIO's MOOC was extensively evaluated for platform usability, learner satisfaction, accessibility, and visual design, gathering feedback from over 295 participants. This is relevant to CyberSecPro as it is committed to creating intuitive, learner-friendly digital environments that support large-scale participation and diverse learner needs, without unnecessary technical barriers.

Evidence-Based Content Development and Iterative Evaluation

The BIBLIO team based their MOOC design on desk research, surveys, and interviews to identify training needs and validated the content with feedback mechanisms like quizzes and participant reflections. This is relevant to CyberSecPro as it also places strong emphasis on research-informed design and continuous evaluation to ensure the content is contextually appropriate, engaging, and effective.

2.1.16 CyberSec4Europe Quality Criteria for Cyber Security MOOCs

The CyberSec4Europe project defines and evaluates quality assurance criteria for cybersecurity MOOCs, including future cyber ranges MOOCs. It also proposes criteria for determining whether such MOOCs merit a quality seal issued by a future European Cybersecurity Competence Network (see Table 20). Fischer-Hübner et al. (2020) report that project partners conducted a pilot evaluation of selected cybersecurity MOOCs by applying a subset of these defined criteria, particularly those specific to cybersecurity. According to the authors, the current landscape lacks dedicated platforms or topic-specific channels for cybersecurity MOOCs. Instead, existing courses are hosted on mainstream learning platforms such as Coursera**,** edX**,** FutureLearn, Udacity, Udemy, and Canvas. Based on their content and structure, cybersecurity MOOCs can generally be categorised into three types:

- *Academic level MOOCs:* These are university-led courses that may offer academic credits and follow formal higher education standards. They are typically open to the public but can also be restricted to enrolled students.
- *Continuous learning MOOCs:* Designed for lifelong learners and professionals, these MOOCs focus on practical cybersecurity skills and are often offered by universities, companies, or NGOs with minimal entry requirements.
- *MOOCs utilising Cyber Ranges:* These combine online learning with hands-on simulations in realistic cyber environments. They involve technical labs to train learners in detecting, mitigating, and responding to cyber threats.

Table 20: CyberSec4Europe MOOC Quality Criteria Based on Fischer-Hübner et al. (2020)

Category	General criteria	Cybersecurity-specific additions
Qualification of the proposer	The proposer must be a recognized institution with experience in MOOC development and delivery.	Recognized by cybersecurity stakeholders; cyber range experience; simulate realistic cyber threats, actors, and environments.
Admission criteria and participant qualification	Admission criteria should be transparent and inclusive.	For cyber range MOOCs, students should either have or acquire skills to operate cyber range platforms.
	Prerequisites should be clearly stated but should not be exclusionary.	
Qualification of instructors	Instructors should have academic or relevant industry qualifications and pedagogical training.	Must be able to manage technical aspects of cyber range operations or work with specialists who can.
Examination, credentialization, and recognition	Exams should fairly assess learning outcomes.	Clear statement on how lab work and cyber range activities contribute to credentials.
	Credentials must reflect achievement and be transparent.	
Course evaluation	Feedback should be collected from students and used for quality improvement. Evaluations should be transparent.	Should involve cybersecurity stakeholders in evaluation follow-ups.
Meeting professional expectations	Engagement with professional stakeholders is encouraged.	Cyber range courses should simulate real operations and

	Course content should reflect real-world needs.	allow participants to apply their own organization's response protocols during exercises.
Course structure and content	Learning outcomes should be clear	N/A
	Content should not be used to market products unless educational.	
Course platform and channels	Platforms must be accessible (EU Directive 2016/2102) and GDPR-compliant.	N/A
Openness	Content should be openly accessible and licensed (e.g., CC-BY-SA).	Any limitation (e.g., due to hacking content) must be justified, transparent, and follow ethical guidelines.
Ethics and privacy	Ethical and privacy policies must be in place and aligned with GDPR.	Courses should "practice what they preach" i.e., demonstrate ethics and privacy in delivery, especially if teaching those concepts.
	Students should not be forced to disclose more personal data than needed.	
Cyber Ranges	Cyber ranges (if used) should offer full support for planning, execution, and analysis.	Requires robust technical and operational infrastructure to simulate real-world cyber defence scenarios.
	Must support teams in detecting, mitigating, and recovering from incidents.	

The Cybersec4Europe project partners applied a subset of the above quality assurance criteria, focusing specifically on those related to cybersecurity, and conducted an exemplary evaluation of six selected cybersecurity MOOCs, namely:

- Continuous learning MOOC: "Information Security: Context and Introduction" by Royal Holloway, UK.
- Continuous learning MOOC: "Managing Security in Google Cloud Platform" by Google.
- Academic MOOC: "Netzwerksicherheit" by Technische Hochschule Lübeck, Germany.
- Academic MOOC: "Privacy by Design" by Karlstad University, Sweden.
- Academic MOOC: "Development of Secure Embedded Systems Specialization", EIT Digital Cybersecurity course.
- Academic and continuous learning MOOC: "Cyber Security Base with F-Secure, Academic", by the University of Helsinki and F-Secure, Finland.

The evaluation procedure for cybersecurity MOOCs in the CyberSec4Europe project followed a structured three-phase approach. First, each MOOC was independently evaluated by five to six project

partners using a predefined set of quality criteria. For each criterion, the reviewers determined whether it was fully met (“yes”), partially met (“partly”), not met (“no”), or if the information was not publicly available (“unclear”). In the second phase, all individual assessments were consolidated into a single evaluation document. Unanimous ratings across reviewers were directly carried over to the combined results. Finally, in the third phase, any discrepancies in the evaluations were resolved through consensus discussions among the reviewers. This allowed the team to finalize the ratings and complete the evaluation of each MOOC.

The evaluations conducted by the Cybersec4Europe project revealed issues regarding the openness of course meta information that restrain evaluators and interested students to assess the quality of MOOCs. Moreover, criteria for assuring privacy, ethical rules for course participants, as well as for ensuring that professional expectations of cybersecurity stakeholders are met, were to a large extent not fulfilled by the selected MOOCs. These shortcomings highlight the need for MOOC designers and developers to proactively address these gaps by ensuring transparency, integrating robust privacy and ethical safeguards, and aligning course content with the expectations of cybersecurity professionals and stakeholders.

The linkage/alignment of CyberSec4Europe framework with CyberSecPro

Cybersecurity-Specific MOOC Quality Criteria

CyberSec4Europe proposes a tailored set of quality assurance criteria specifically for cybersecurity MOOCs, including those using cyber ranges. This is relevant to CyberSecPro since it is a cybersecurity-focused project that requires discipline-specific quality standards to ensure its training offer is fit-for-purpose, secure, and professionally recognised.

Evaluation Categories Addressing Ethical, Legal, and Technical Aspects

The framework expands traditional MOOC QA dimensions with criteria on privacy, ethics, cyber range functionality, and realistic simulation design. This is relevant to CyberSecPro as it includes technical, potentially sensitive topics and real-world application exercises, where ethical and privacy concerns are crucial and must be integrated into course design and delivery.

Support for a Governance Model and a Quality Seal

The framework includes a structured peer-review-based evaluation procedure and governance model for awarding a quality seal to cybersecurity MOOCs. This is relevant to CyberSecPro as it is part of a European initiative that seeks sustainability, credibility, and mutual recognition of its microcredentials, for which a robust QA and certification model is essential.

Focus on Stakeholder Involvement and Professional Expectations

CyberSec4Europe emphasises the inclusion of stakeholders from industry, government, and ethical hacking communities in the course evaluation process. This is relevant to CyberSecPro as it engages with external partners to align its training with labor market needs and ensure relevance for current cybersecurity professionals.

Integration with European Standards and GDPR Compliance

The framework ensures alignment with EU-level quality assurance standards (e.g., ISO/IEC 40180, OpenupEd QL, GDPR). This is relevant to CyberSecPro since it must comply with European regulations and frameworks in order to ensure the legal soundness and institutional acceptance of its digital learning pathways.

2.1.17 European MOOC Consortium Labour Market (EMC-LM)

The framework was developed under the European MOOC Consortium - Labour Markets (EMC-LM) project to ensure the quality, credibility, and recognition of micro credentials delivered via MOOC platforms. It builds on the Common Micro credential Framework (CMF) and the prior compendium of good practices in ID verification, assessment, and recognition.

This evaluation framework is designed to be practical and reflective, guiding course providers in aligning their micro credentials with European standards. It includes two core checklists, each divided into dimensions and criteria, to assess the following:

1. Extent to which the learning experience enables a recognized CMF micro-credential.
2. Extent to which assessment and recognition follow best practices.

Each criterion is rated using a 4-point scale:

- NA (Not achieved)
- PA (Partially achieved)
- LA (Largely achieved)
- FA (Fully achieved)

There is also room for reflective comments, making this both a quantitative and qualitative tool. The criteria for EMC-LM framework assessment are defined below.

Table 21: EMC-LM Assessment Criteria by Iniesto (2021)

Dimension	**Criteria**	**Assessment and recognition**			
		NA	PA	LA	FA

ID verification	The course operates a reliable method of ID verification at the point of assessment that complies with the recognized University's policies or is widely adopted across platforms using (more than one could be used). Methods defined as "basic" should be accompanied by another method marked as "good" or "better" to grant verification for full achievement:
	• Platform ID verification (Basic)
	• Provider registration (Basic)
	• Interviews:
	  ○ On-site oral interviews (Basic)
	  ○ Online interviews (Good)
	• Recorded presentations (Better)				

	Comments:				

	The ID verification method has been checked as accessible for participants with accessibility needs.				
	Comments:				
Assessment	The course provides a summative assessment to enable the awarding of academic credit via recognition of prior learning upon enrolment for specified qualifications offered by the course provider.				
	Comments:				
	The summative assessment (s) has been checked as accessible for participants with accessibility needs.				
	Comments:				
Accreditation and recognition	The course provides at least a method for recognition: • Academic Credit: Formal and transferable • Professional Credit: Formal and endorsement • Combined: Academic and professional				
	Comments:				
	The course should be awarded in a digital and signed format, for example, the identified Europass Digital Credentials (EDC).				
	Comments:				
	The course provider has a strategy that addresses recognition of micro-credentials.				
	Comments:				
	The transcript issued in a widely spoken language or an easy-to read graphical format, in a standardized form, according to standardized processes				
	Comments:				
QA framework	The quality is assured by passing the normal provider quality assurance processes: • The course offers academic credit and is quality assured using the same procedures that are used for other courses for academic credit offered by the institution				

	• The course offers professional credit and is quality assured using the same procedures that are used for other courses offering similar professional credit				
	Comments:				
	The provider of the course applies internal quality assurance mechanisms following internal quality criteria and procedures.				
	Comments:				

The linkage/alignment of EMC-LM Framework with CyberSecPro

Alignment with Labor Market Needs

The EMC-LM framework is highly relevant to CyberSecPro because both initiatives aim to address labor market needs through tailored education. EMC-LM was established to align microcredential offerings (particularly MOOCs) with the skills demanded by employers across Europe. Similarly, CyberSecPro seeks to close the cybersecurity skills gap by equipping learners with job-ready competencies. By focusing on employability, both projects contribute to bridging the gap between formal education and professional requirements, making EMC-LM a strategic reference for CyberSecPro's development goals.

Microcredential Development and Recognition

A key output of EMC-LM is its comprehensive framework for the assessment and recognition of microcredentials. This framework ensures that credentials are credible, portable, and aligned with standards such as the European Qualifications Framework (EQF) and the European Credit Transfer and Accumulation System (ECTS). For CyberSecPro, which also intends to issue microcredentials in the cybersecurity domain, adopting or adapting this framework helps ensure that the credentials are recognised by higher education institutions and employers alike. The EMC-LM model provides CyberSecPro with a tested methodology for quality assurance and validation of learning outcomes.

Support for Lifelong and Flexible Learning

Both EMC-LM and CyberSecPro promote the value of short, flexible, and stackable learning opportunities. This approach is especially valuable for adult learners and professionals who need to balance upskilling with other responsibilities. EMC-LM framework highlights how microcredentials can be designed to support personalised and modular learning journeys. For CyberSecPro, this model supports the creation of a cybersecurity training pathway that accommodates learners at various career stages and enables progression across levels. The emphasis on stackability and flexibility aligns with modern trends in digital learning and workforce development.

2.1.18 EMMA Evaluation Methodology

The EMMA Evaluation Methodology was developed by the European Multiple MOOC Aggregator (EMMA) Project. The methodology is used to systematically assess the quality and effectiveness of both the EMMA platform and the individual MOOCs it hosts. Evaluation is conducted through a combination of structured learner surveys, learning analytics, and digital trace data.

When a learner registers, they complete a registration questionnaire that captures demographic details and learning backgrounds. Upon enrolling in a course, they complete a pre-course questionnaire to

express expectations and motivations. At the end of the course, they are asked to complete an exit questionnaire to evaluate their satisfaction, perceived learning gains, and reasons for potential dropout.

These survey responses are then combined with behavioural data (such as course activity, content accessed, progress made) through a unique user ID. This integration allows evaluators to track each learner's journey, analyse learning patterns, and distinguish between different types of learners (e.g., active vs. passive participants).

The resulting data informs improvements at two levels:

- Course level: instructors receive feedback to revise content, structure, or pedagogy.
- Platform level: developers use usability insights and usage patterns to refine the system's functionality and learner support services.

The methodology is designed to be iterative, enabling ongoing improvements after each evaluation cycle based on real user feedback and engagement data. It is important to mention that the framework was not developed for a specific discipline. It is intended to be used across diverse MOOCs from different academic fields (Ferrari et al., 2014). For example, EMMA was piloted with MOOCs in various subjects, and the evaluation framework was designed to handle this disciplinary diversity through a combination of standard and customizable evaluation instruments.

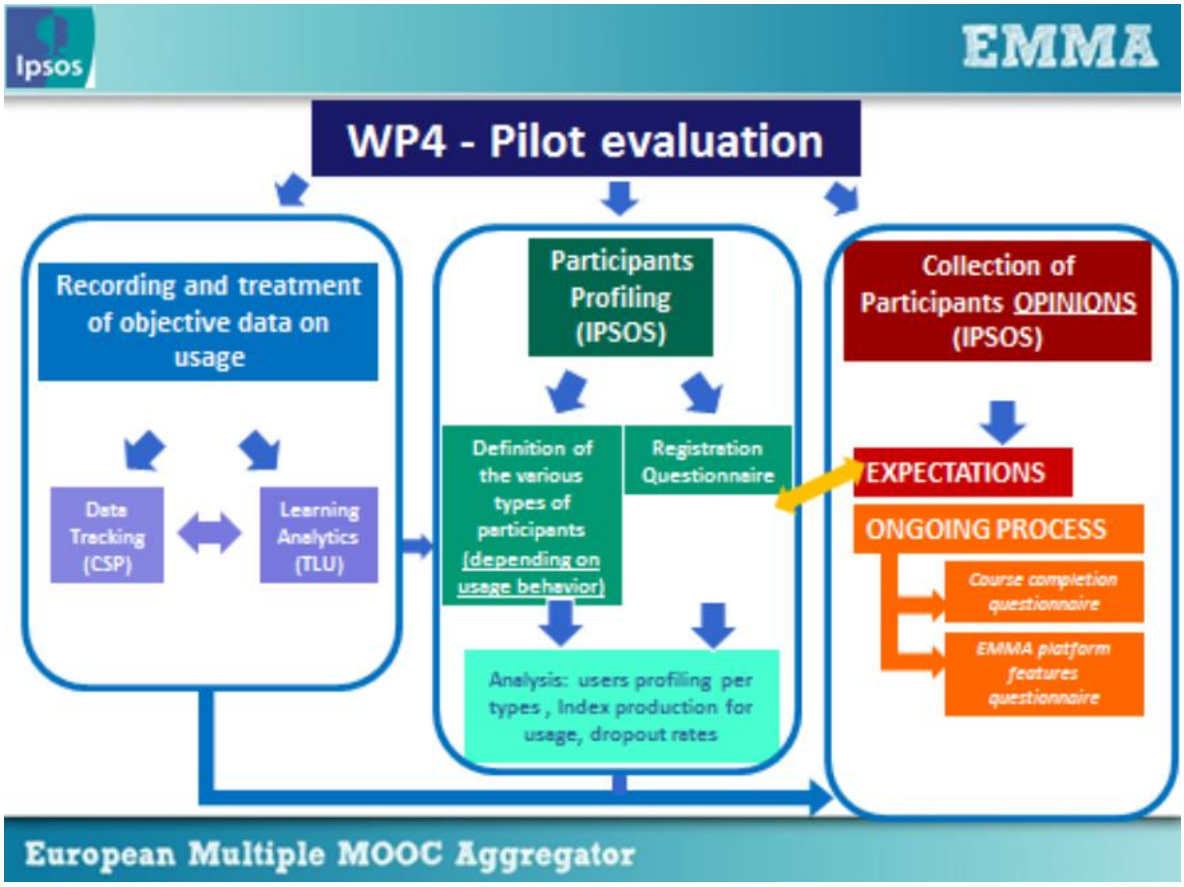

Figure 3: European Evaluation Methodology by Ferrari et al. (2014)

The linkage/alignment of EMMA Framework with CyberSecPro

Comprehensive Evaluation Framework Combining Learning Analytics and Surveys

The EMMA project developed a dual-layer evaluation methodology that merges digital learning analytics with structured learner feedback through entry, expectation, and exit questionnaires. This is relevant to CyberSecPro as it integrates both platform usage data and learner-reported insights to monitor engagement, personalise feedback, and continuously improve the effectiveness of cybersecurity MOOCs.

Support for Adaptive, Iterative Course Improvement

The evaluation system in EMMA is designed for iterative application—allowing course providers to adjust MOOC design based on user satisfaction and interaction patterns in real time. This is relevant to CyberSecPro as it follows an iterative development model and must respond dynamically to learner behavior, technical feedback, and platform usability issues to improve training outcomes.

Clustering Learner Types to Analyse Behaviour and Experience

EMMA defines detailed learner clusters (e.g. passive, active, drop-in, non-starters) to analyse how different types of users engage with MOOCs. This is relevant to CyberSecPro as it seeks to understand diverse learner pathways in cybersecurity, especially important in designing content that suits varying engagement levels and professional needs.

Multilingual and Multicultural Platform Considerations

EMMA emphasises a multilingual, multicultural approach, including translation and user language tracking during evaluation. This is relevant to CyberSecPro as it delivers training across Europe and must ensure that language accessibility, cultural diversity, and localisation are factored into platform evaluation and learner satisfaction.

Focus on Learner Profiling and Satisfaction as Success Metrics

The EMMA framework places strong emphasis on user profiling, tracking expectations, and measuring satisfaction through detailed surveys. This is relevant to CyberSecPro as it aims to demonstrate the value and impact of its microcredentials not just through completion rates but through learners' perceived quality, relevance, and usability of the training.

2.1.19 MICROBOL Common Framework for Micro-credentials

The MICROBOL project developed a common European framework for micro-credentials aligned with the Bologna Key Commitments (QF-EHEA, ECTS, recognition, and quality assurance). The framework builds on existing EHEA tools but adapts or reinterprets them to accommodate the unique characteristics

of micro-credentials (e.g., modularity, stackability, digital delivery). The framework is informed by prior European projects (e.g., MicroHE, e-SLP, OpenupEd) and international efforts (e.g., from the U.S., Australia, and New Zealand).

The MICROBOL report (2020) suggests that the framework is designed to be cross-disciplinary and is not limited to a specific field. It is applicable to a wide range of micro-credentials, including those offered via MOOCs, professional/industrial certificates, academic short courses, badges, and nanodegrees. It can be used for micro-credentials in both academic and non-academic contexts, such as continuing education, workforce training, and lifelong learning.

Table 22: MICROBOL Common Framework for Micro-Credentials Based on Cirlan et al. (2020)

Component	Evaluation focus	How it can be used
Qualification framework (QF-EHEA)	Level alignment	Micro-credentials should map to QF-EHEA levels (e.g., Bachelor, Master) using defined learning outcomes and competency descriptors.
ECTS	Workload and credit transparency	Micro-credentials should be assigned ECTS credits based on estimated workload (typically 4–6 ECTS = 100–150 hours) and allow credit accumulation.
Recognition (Lisbon Recognition Convention)	Transparency and comparability	Micro-credentials must provide clear information on workload, level, learning outcomes, and assessment to support recognition and credit transfer.
Quality assurance (ESG)	Internal and external quality assurance	Institutions must align with ESG standards: define learning outcomes, assessment methods, and ID verification; maintain public access to course info.
Transcripts and metadata	Documentation and portability	Micro-credentials should include transcripts detailing learning outcomes, credit points, level, and workload; preferably issued in digital formats (e.g., Europass, Open Badges).

The linkage/alignment of MICROBOL Framework with CyberSecPro

Integration with Bologna Process and EHEA Tools

The MICROBOL report focuses on how existing Bologna Process tools—like the Qualifications Framework for the EHEA (QF-EHEA), ECTS, the Lisbon Recognition Convention, and the Standards and Guidelines for Quality Assurance (ESG)—can be used or adapted for micro-credentials. This is relevant to CyberSecPro as it is an EU-funded initiative grounded in the Bologna framework and must ensure that its cybersecurity microcredentials align with European recognition, credit transfer, and quality assurance mechanisms.

Emphasis on Stackability, Portability, and Recognition

The report identifies stackability, portability, and transparency as defining characteristics of high-quality micro-credentials. This is relevant to CyberSecPro as it seeks to develop modular, stackable training pathways that support lifelong learning and can be recognized across national and institutional contexts throughout the EU.

Clarification of ECTS Workload and Leveling Requirements

MICROBOL outlines how micro-credentials can be defined in terms of workload (e.g. 4–6 ECTS), learning outcomes, and qualification levels (EQF levels 5–8). This is relevant to CyberSecPro as its courses must be precisely described in terms of effort, level, and outcomes in order to be credible, interoperable, and usable for credit accumulation or transfer.

Focus on Trust, Transparency, and Quality Assurance

The report underscores the importance of quality assurance aligned with the ESG, and the need for clear, verifiable, and consistent documentation of learning outcomes, assessment, and delivery. This is relevant to CyberSecPro as it aims to deliver trustworthy cybersecurity education that meets quality benchmarks, supports learner mobility, and builds institutional and employer confidence in its credentials.

Bridging Formal and Non-Formal Learning

MICROBOL supports a flexible approach to micro-credentials that recognizes both formal and non-formal learning contexts, such as MOOCs and digital badges. This is relevant to CyberSecPro as it operates across diverse educational environments and must ensure that its microcredentials, while often delivered via MOOCs, are robust enough to be integrated into formal qualification pathways or professional recognition systems.

2.1.20 OpenupEd Quality Assurance Spectrum

The OpenupEd initiative developed a set of quality assurance checklists for MOOCs based on the ECO and SCORE2020 project. The checklists assess compliance with established norms and shifts the focus from product-oriented quality to systems that enhance quality through process-based approaches. While most existing QA systems for MOOCs are characterized by externally set standards, the OpenupEd Label encourages institutions to embed internal processes aimed at continuous quality improvement aligned with their own objectives. The checklist enables MOOC providers with a basic framework to self-assess the following aspects (Table 23-26):

- Whether their offerings meet the definition of a MOOC
- The quality of MOOC design
- Accessibility
- The technical platform and the support for both staff and participants.

MOOC providers interested in becoming OpenupEd partners are expected to complete the checklist and submit it along with an official letter of intent. New partners are required to achieve the OpenupEd Label within three years of joining the initiative.

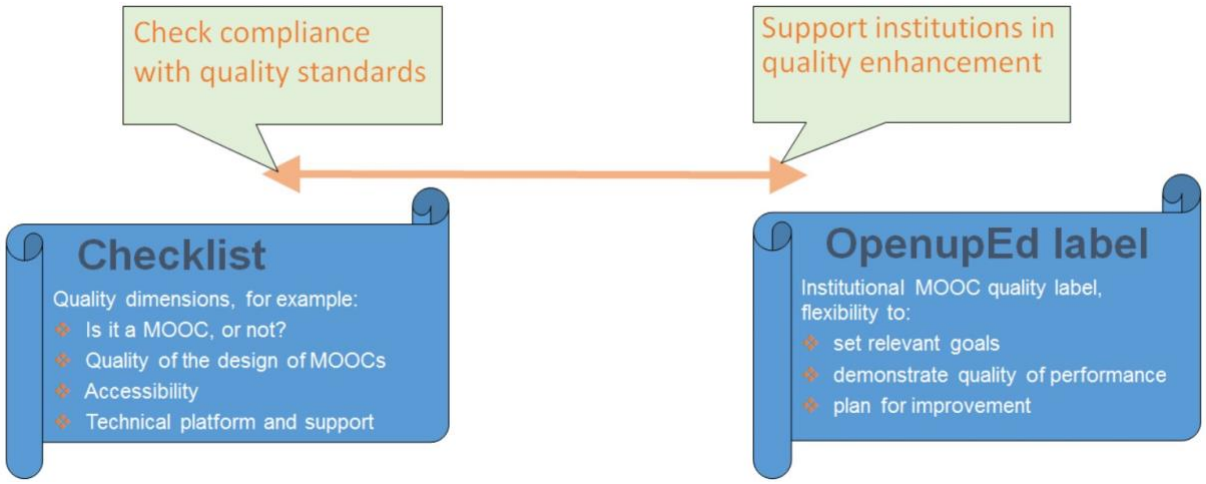

Figure 4: OpenupEd Quality Assurance Spectrum by SCORE2020 Project (2020)

Table 23: Checklist for Determining MOOC Definition by SCORE2020 Project (2020)

Dimension	Criteria	Is it a MOOC, or not?			
		NA	PA	LA	FA
Massive	The (pedagogical model of the) course is such that the efforts of all services (including of academic staff on tutoring, tests, etc.) does not increase significantly as the number of participants increases	☐	☐	☐	☐
Open	Course accessible to (almost) all people without limitations	☐	☐	☐	☐
	At least the course content is always accessible	☐	☐	☐	☐
	The course can be accessed anywhere as long as someone has an internet connection	☐	☐	☐	☐
	No qualifications / diplomas needed to participate in the online course	☐	☐	☐	☐
	Full course experience without any costs for participants	☐	☐	☐	☐
Online	All aspects of the course are delivered online	☐	☐	☐	☐
Course/study unit	The total study time of a MOOC is at minimum 1 ECTS (25–30 hours of study)	☐	☐	☐	☐
Full course	The course provides a complete learning experience with content that may include video, audio, text, games (including simulations), social media, and animations	☐	☐	☐	☐
	The course offers possibilities for interaction, such as social media channels, forums, blogs, or RSS readers to build a learning community	☐	☐	☐	☐
	Participants are provided with some feedback mechanism. It can be automatically generated (e.g., quizzes), offered by peers or general feedback from academic staff, etc.	☐	☐	☐	☐
	Always includes some kind of recognition like badges or a certificate of completion. A formal certificate is optional and most likely has to be paid for	☐	☐	☐	☐
	A study guide / syllabus includes instructions as to how you may learn from the presented materials and interactions	☐	☐	☐	☐

Rubric: NA (Not achieved); PA (Partially achieved); LA (Largely achieved); FA (Fully achieved)

Table 24: Quality Checklist for MOOC Design by SCORE2020 Project (2020)

Dimension	Criteria	Design of MOOC			
		NA	PA	LA	FA
Target group	MOOCs are accessible to all people and, as such, various target groups are identified	☐	☐	☐	☐
	For each target group, the needs, challenges and prior knowledge are described	☐	☐	☐	☐
	The description of each target group is supported by references to different studies	☐	☐	☐	☐
Goal	The overall objective of the course is described in a few sentences	☐	☐	☐	☐
Learning objectives	The course describes a limited number of learning objectives	☐	☐	☐	☐
	Clear statements of learning outcomes for both knowledge and skills are provided	☐	☐	☐	☐
	There is reasoned coherence between learning outcomes, course content, teaching and learning strategy (including use of media), and assessment methods	☐	☐	☐	☐
	The prior knowledge of each learning objective is described and related to the characteristics of target groups	☐	☐	☐	☐
Learning activities	Activities aid participants to construct their own learning and to communicate it to others	☐	☐	☐	☐
	The “pathways” (activities, tasks, and routes) are designed in such a way that they can be performed at different levels of difficulty or complexity, to account for the broad spectrum of participants’ knowledge and skills that is expected	☐	☐	☐	☐
	Various activities are proposed with different formats. For example: quizzes, peer-to peer evaluation, video conferences (Google+/Hangouts), activities in the forums and platform social networks or external social networks (Facebook, X, Bluesky)	☐	☐	☐	☐
	The MOOC contains differing levels of difficulty, with different learning pathways	☐	☐	☐	☐

	The course contains sufficient interactivity (learner-to-content, learner-to-learner or learner-to-teacher) to encourage active engagement	☐	☐	☐	☐
Feedback mechanism	Feedback by an academic tutor is limited and scalable (characteristic of MOOC)	☐	☐	☐	☐
	The course provides learners with regular feedback through self-assessment activities, tests or peer feedback	☐	☐	☐	☐
	The frequency of monitoring has been planned (forum, group, post).	☐	☐	☐	☐
	A weekly announcement or massive mailing with orientations for the following week is planned.	☐	☐	☐	☐
	In each weekly session, the pedagogical team makes a synthesis of artefacts from the previous week's session	☐	☐	☐	☐
	Some live events (Hangout, Tweetchat) are scheduled	☐	☐	☐	☐
Study-time	The total study time of all learning activities (including quizzes, tests, and exam) is at minimum 1 ECTS (25–30 hours of study)	☐	☐	☐	☐
Workload	The schedule of the course is such that the workload per week is feasible for typical learners from the specified target group (typical 6–8 hours for those with full-time jobs)	☐	☐	☐	☐
	The MOOC is realistic in its pacing for the participants, accommodating to the individual's personal rhythm	☐	☐	☐	☐
Assessment	Learning outcomes are assessed using a balance of formative and summative assessment appropriate to the level of certification	☐	☐	☐	☐
	Assessment is explicit, fair, valid, and reliable. Measures appropriate to the level of certification are in place to counter impersonation and plagiarism	☐	☐	☐	☐
	Participants can earn badges for completion of learning activities	☐	☐	☐	☐
	The MOOC has possibilities to follow the score and progression	☐	☐	☐	☐

Rubric: NA (Not achieved); PA (Partially achieved); LA (Largely achieved); FA (Fully achieved)

Table 25: Quality Checklist for Accessibility of MOOCs by SCORE2020 Project (2020)

Dimension	**Criteria**	**Design of MOOC**			
		NA	PA	LA	FA
Web accessibility	Compliant to W3C accessibility	☐	☐	☐	☐
	Compliant to WCAG 2.0 according to the European Commission	☐	☐	☐	☐
Accessible information	Implemented the Guidelines for Accessible Information	☐	☐	☐	☐
Accessible learning	The introduction videos are subtitled / transcribed	☐	☐	☐	☐
	Participants can download resources, as to store, and use them without an internet connection	☐	☐	☐	☐
	Implemented the Guidelines from Universal Design for Learning	☐	☐	☐	☐

Rubric: NA (Not achieved); PA (Partially achieved); LA (Largely achieved); FA (Fully achieved)

Table 26: Quality Checklist for Technical Staff Based on SCORE2020 Project (2020)

Dimension	Criteria	Design of MOOC			
		NA	PA	LA	FA
Platform	The MOOC platform is reliable, secure and assures appropriate levels of privacy. Provision is made for system maintenance, monitoring, and review of performance	☐	☐	☐	☐
	The MOOC platform provides a range of online tools which are appropriate for the educational models adopted	☐	☐	☐	☐
Staff support	The institution provides appropriate training for academic and support staff to develop the skills required to develop and deliver MOOCs	☐	☐	☐	☐
	The institution provides adequate support and resources to MOOC staff and manages workloads appropriately	☐	☐	☐	☐
	MOOC participants are provided with clear and up-to-date information about courses including aims/objectives, learning and assessment methods, workload and prerequisite knowledge	☐	☐	☐	☐
Support for MOOC participants	Participants have access to their personal learning environment, follow progression, tasks, completion, badges, and publications	☐	☐	☐	☐
	The institution uses social networking media to foster academic communities among MOOC participants	☐	☐	☐	☐
	MOOC participants have clear routes to academic, technical and administrative support	☐	☐	☐	☐
	The participant assisted by a technical guide for good navigation	☐	☐	☐	☐
	A FAQ is in place to support participants navigation	☐	☐	☐	☐
	The participant is assisted by pedagogical guidelines for good learning	☐	☐	☐	☐
	A list of criteria for the learning activities, specifically for peer-to-peer evaluations, is available	☐	☐	☐	☐

Rubric: NA (Not achieved); PA (Partially achieved); LA (Largely achieved); FA (Fully achieved)

The linkage/alignment of OpenupEd Framework with CyberSecPro

Use of Structured, Self-Assessment-Based QA Checklists for MOOCs

The OpenupEd QA framework provides a detailed set of checklists covering MOOC definition, design, accessibility, platform reliability, and learner support, with a four-point scoring system (NA–FA). This is relevant to CyberSecPro as it is committed to systematically assuring the quality of its cybersecurity microcredentials, and needs practical tools to benchmark course development across diverse institutional partners.

Grounding in Higher Education QA Norms and Principles

The checklists are built upon existing HE quality assurance standards and promote institution-embedded quality enhancement processes rather than externally imposed norms. This is relevant to CyberSecPro as it operates within the European Higher Education Area (EHEA) and must ensure that its quality model is both academically credible and adaptable to varied institutional contexts.

Emphasis on Inclusive Course Design and Accessibility Standards

OpenupEd includes a dedicated checklist for web accessibility, accessible information, and Universal Design for Learning (UDL) compliance. This is relevant to CyberSecPro as it delivers digital training to a diverse, Europe-wide audience, and must ensure that all learners, regardless of physical ability or digital literacy level, can fully participate in and benefit from the learning experience.

Support for Participant-Centered Learning and Interactivity

The framework assesses whether courses include interactive learning activities, multiple difficulty levels, peer collaboration, and feedback mechanisms. This is relevant to CyberSecPro as it prioritizes active, applied, and collaborative learning approaches in cybersecurity education, where hands-on problem-solving and teamwork are essential for skill development.

Technical Infrastructure and Staff Support Considerations

The checklists address the technical robustness of MOOC platforms, training and support for academic staff, and clear guidance and resources for learners. This is relevant to CyberSecPro as it requires reliable digital infrastructure, effective instructional capacity-building, and responsive learner support systems to successfully deliver high-impact cybersecurity micro credentials at scale.

2.2 Key Similarities and Considerations for CyberSecPro Evaluation Methodology

The analysis of the frameworks above highlights several common points essential for developing a robust evaluation methodology for CyberSecPro. These similarities emphasize learner-centred design, quality assurance, assessment authenticity, and alignment with European standards. The following points outline key considerations to integrate into CyberSecPro's evaluation approach.

1. **Learner-Centred Design**

   Emphasis on active learning, flexibility, autonomy, and diverse learning needs. Personalized pathways and inclusive design (e.g., Bali (2014), Sebbaq & El Faddouli (2024), Shah et al. (2023), EMMA Framework, Yılmaz et al. (2017)).

2. **Multi-Dimensional Quality Assurance**

   Use of structured frameworks covering multiple aspects such as pedagogy, technology, assessment, and usability. Examples: Chan's 8 dimensions, Stracke's QRF, Poce's rubric, Shah's MEF, Sabjan's 3 dimensions.

3. **Use of Learning Analytics and AI**

   Integration of data-driven insights (e.g., engagement metrics, behaviour tracking) to improve course delivery. AI tools to automate evaluation and personalize learning (Chan (2023), Tzeng et al. (2022), EMMA Framework, Duan & Wu (2023)).

4. **Authentic and Diverse Assessment**

   Promotion of formative, reflective, real-world, or peer-reviewed assessments over simple quizzes or completion rates. Examples: Bali (2014), Duan & Wu (2023), Sebbaq & El Faddouli (2024), OpenupEd approach.

5. **Iterative, Continuous Improvement**

   Frameworks support formative evaluation cycles and agile course updates based on feedback and data (EMMA Framework, Stracke et al. (2018), Poce et al. (2019), Shah et al. (2023)).

6. **Alignment with European QA and Recognition Standards**

   Many frameworks align with ENQA, ESG, ECTS, EQF, MICROBOL, and OpenupEd standards. Relevant for credibility, portability, and stackability of micro credentials (Ferreira et al. (2022), MICROBOL, CyberSec4Europe, EMC-LM framework).

7. **Support for Modular, Scalable Learning**

   Frameworks favour modular design (e.g., subMOOCs, stackable units), suitable for lifelong learning and large-scale delivery (BIBLIO, MICROBOL, OpenupEd, Shah et al. (2023)).

8. **Stakeholder and Contextual Relevance**

   Need to align MOOC design and evaluation with learner needs, employer expectations, and institutional goals (Douglas et al. (2019), CyberSec4Europe, EMC-LM framework).

9. **Emphasis on Inclusivity and Accessibility**

Frameworks encourage consideration for multilingualism, low-bandwidth formats, accessibility standards (Bali (2014), Yılmaz et al. (2017), OpenupEd, EMMA Framework).

10. Technological Infrastructure and Usability

Evaluation of platform reliability, user interface, and learner support services (BIBLIO, OpenupEd, Shah et al. (2023), Yılmaz et al. (2017)).

3 CyberSecPro Evaluation Context

The evaluation framework developed for CyberSecPro reflects the project's ambition to deliver high-quality, impactful, and practice-oriented cybersecurity training aligned with European standards. It seeks to ensure that the MOOCs and training modules not only meet technical expectations but also support pedagogical relevance and business applicability.

Evaluation Objectives

The key objectives of the evaluation are to:

- Assess the impact of the training on learners' satisfaction, confidence, and workplace application
- Evaluate the usability and accessibility of platforms and learning tools
- Ensure the quality and coherence of the training materials across technical, pedagogical, and business dimensions.

Evaluation Scope

The evaluation covers the entire cycle of course design, delivery, and refinement. It includes feedback from trainers and providers, captures usability and engagement data, and considers how the training translates into practical outcomes for learners.

Difference from WP3 Surveys

Unlike the short-term feedback mechanisms in WP3, which focus primarily on the achievement of learning outcomes, WP5's evaluation framework emphasises broader performance indicators (especially satisfaction measures) and (expected) long-term impact. It is designed to enable benchmarking, quality assurance, and continuous improvement at the Module and overall CSP training level.

Flexibility and Depth

A key challenge addressed in this evaluation is balancing depth and extensiveness. To avoid overburdening trainers and trainees and overlapping with the existing evaluation, flexibility is built into the survey design, allowing partners to tailor and prioritise specific elements based on local implementation contexts. This ensures meaningful data collection without compromising comparability across partners.

Future Use and Transferability

The evaluation methodology and instruments are designed for reuse beyond the CyberSecPro project. By aligning with recognised standards and good practices, the tools can be adapted by other institutions and training providers seeking to assess cybersecurity education programs effectively.

4 Evaluation of Training Implementation

The evaluation methodology developed in Task 5.1 has a distinct focus and purpose. While the previous survey (WP3) aimed to gather feedback on the module's effectiveness in terms of achievements of learning outcomes, this evaluation is centred on two key aspects: assessing learner satisfaction with the training activities and examining the trainer's experience in developing and delivering the module using the provided training materials. Ultimately, the goal is to inform future improvements and provide recommendations for both training material developers and prospective trainers. This chapter presents the evaluation approach for both target groups, namely trainers and trainees.

4.1 Evaluation by Trainees

4.1.1 Criteria / KPIs (Technical, Pedagogical, and Business)

Based on the review of existing frameworks (Chapter 2) as well as the CyberSecPro context (Chapter 3), the following questions have been developed. Please also refer to Appendix A for an overview of which existing frameworks have guided the development of these questions.

Table 27: Questions for Survey to be Filled in by Trainees

Criteria	Question		Scale	Technical	Pedagogical	Business
Overall satisfaction	How would you rate your overall satisfaction with the training module?		7-point Likert scale	x	x	x
Course content and structure	How satisfied are you with …	the overall quality of instructional materials?	7-point Likert scale		x	
		the clarity of instructional materials?	7-point Likert scale		x	

		the practical relevance of the content (e.g. needed practical skills, real-world scenarios, professional contexts, and industry standards)?	7-point Likert scale			x
		the alignment of course design and content with the intended learning objectives?	7-point Likert scale		x	
Instructor	How satisfied are you with …	the instructor's knowledge and competence brought into the training module?	7-point Likert scale		x	
		the instructor's responsiveness and support?	7-point Likert scale		x	
		the instructor's teaching approach?	7-point Likert scale		x	
Learning platform	How satisfied are you with …	the accessibility of the learning platform?	7-point Likert scale	x		
		the ease of navigation of the learning platform?	7-point Likert scale	x		
		the performance and reliability of the platform (e.g. no errors and quick loading times)?	7-point Likert scale	x		
		the visual appeal of the platform?	7-point Likert scale	x		

		the interactivity and engagement of opportunities on the platform (e.g., quizzes, discussion forums, gamification)?	7-point Likert scale	x		
Community & interaction	How satisfied are you with …	the interactions facilitated between learners and external actors (e.g. invited experts)	7-point Likert scale		x	x
		the interactions facilitated between learners	7-point Likert scale		x	
Evaluation & recognition	How satisfied are you with …	the transparency of the examination process?	7-point Likert scale		x	
		the fairness of the examination process?	7-point Likert scale		x	
		the value the (attendance) certificate provides in your professional or academic field?	7-point Likert scale		x	
Impact on students	How relevant are the skills and knowledge gained to your current or desired job role?		7-point Likert scale			x
	To what extent did this course enhance your knowledge and skills?		7-point Likert scale		x	
	How likely are you to further explore the topic of the module (e.g. through self-learning or another course)?		7-point Likert scale	x	x	x

Recommendation	How likely are you to recommend this learning experience to someone looking to improve skills in the cybersecurity field?	Net Promoter Score		x	x
	How could the overall learning experience be enhanced?	Open text field		x	
	Any further comments you like to share?	Open text field	x	x	x

4.1.2 Instruments / Tools

The evaluation, from the learner's perspective, is conducted using a digital survey tool integrated within the CSP Admin Portal. This dedicated feature, titled “Evaluation Survey”, allows trainers of each module to independently design and customise their own evaluation forms.

To create the evaluation, trainers first select the specific module they wish to evaluate. The system then enables them to choose from a pool of pre-defined questions tailored to assess various aspects of the training, including course content and structure, instructor, learning platform, community/interaction, evaluation and recognition, impact, and final insights. This flexibility and modularity ensure that the evaluation aligns closely with the unique structure and goals of each module.

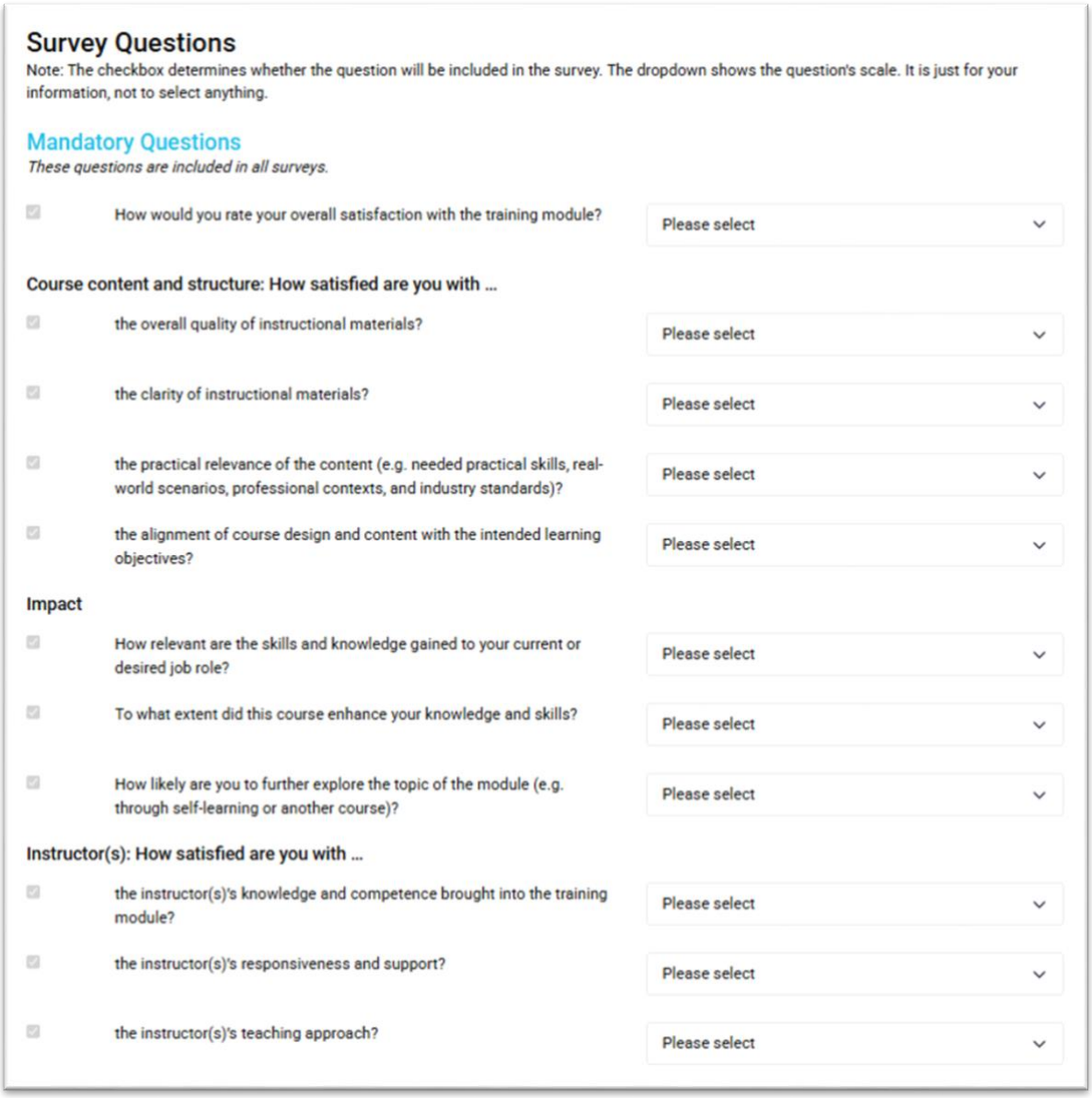

Figure 5: Screenshot of the Survey Builder in the CSP Admin Platform

Once the evaluation form is finalized, a unique URL and a QR code is automatically generated, both of which can be used by trainees to access the survey. These sharing tools facilitate easy and quick distribution of the evaluation form across various digital platforms, including email, chat, or presentation slides during the training sessions.

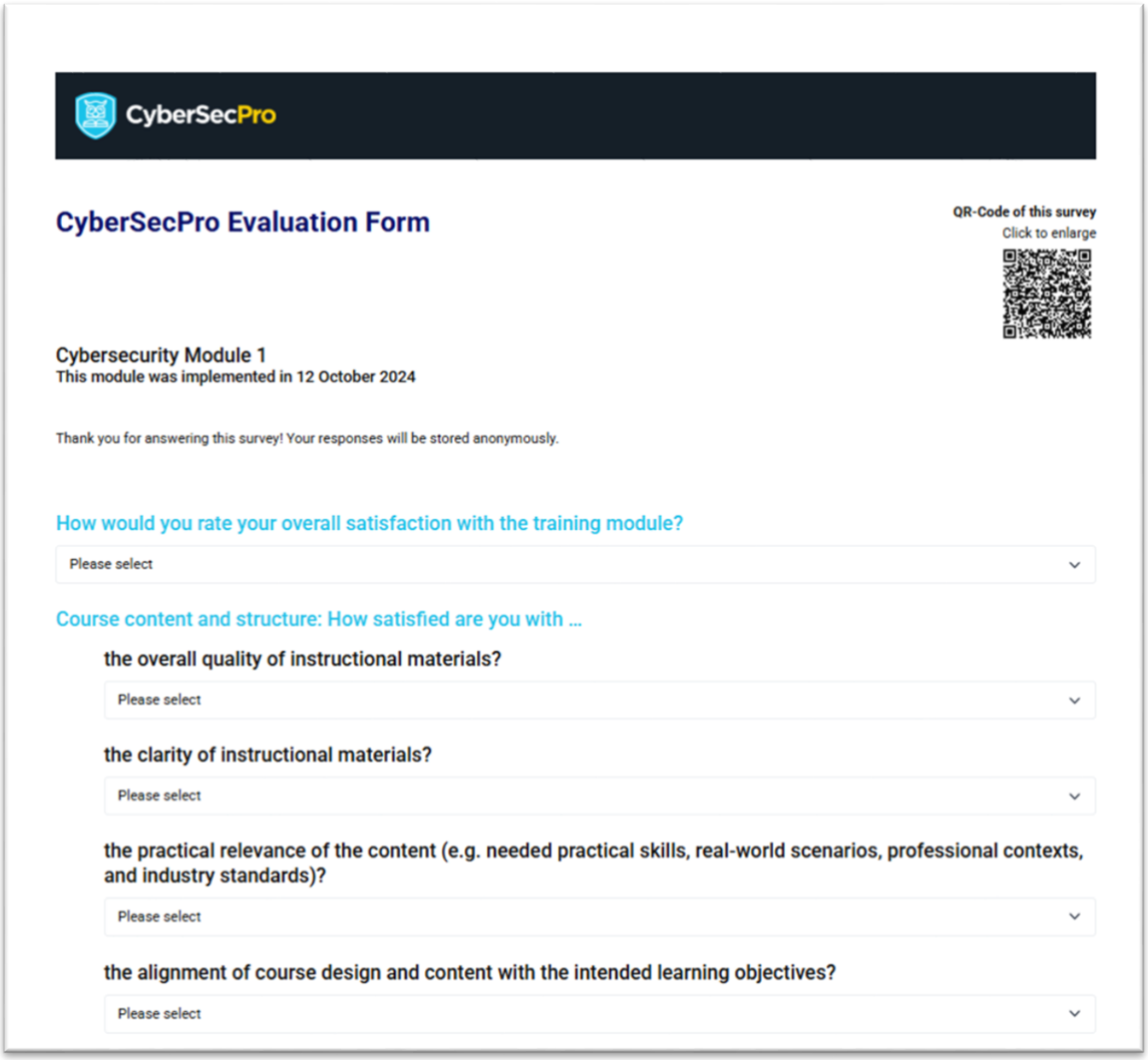

Figure 6: Survey Form for Trainees to Fill, incl. QR Code

4.1.3 Data Collection and Analysis Process

The data collection process is streamlined and entirely digital. Trainers shared the QR code or URL link generated by the CSP Admin Portal with their respective trainees. This allows learners to complete the evaluation survey using their own devices, either during or after the training session.

Once submitted, all responses are stored securely on ACEEU's central server, ensuring data privacy and easy accessibility for analysis. The CSP Admin Portal is equipped with basic analytics functionalities, which enable the aggregation and visualisation of the collected data.

For a high-level analysis (real-time), we utilise bar charts to represent trainee feedback across different dimensions. These visualisations facilitate a quick overview of strengths and potential areas for improvement in each module. Deeper analysis will be performed in Task 5.2.

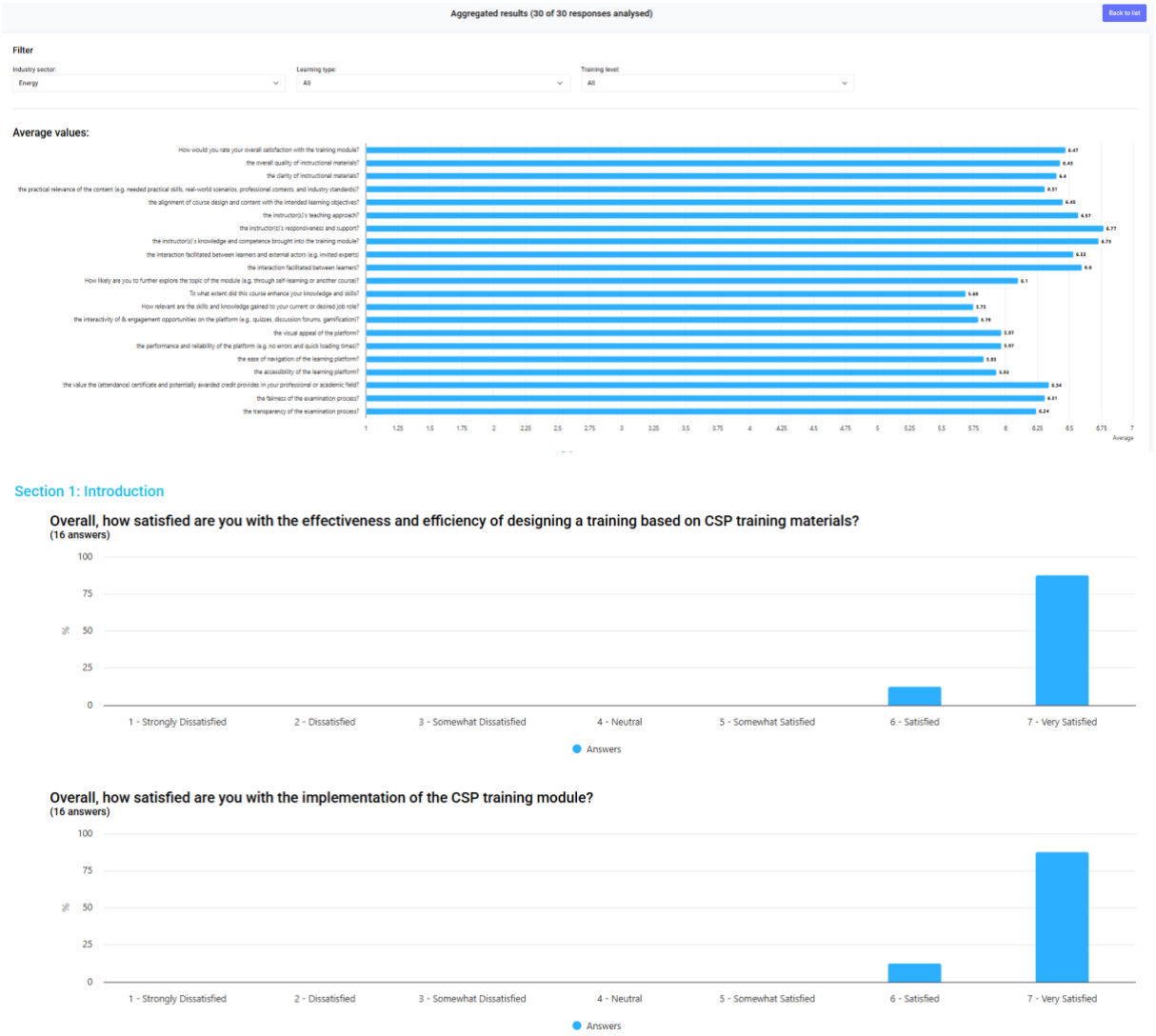

Figure 7: Visualization of Aggregated Results and Statistics from Survey for Trainees

The use of standardised tools and a centralised data management system contributed to the consistency, reliability, and efficiency of the evaluation process.

The data analysis functions of the platform are continuously advanced based on feedback from CSP partners, especially with more data being stored and new insights being gained. The ultimate goal is to continue advancing the platform to be able to provide real-time analysis results that can be used by trainers (e.g. discussing it with learners right away), content developers, CSP consortium members, and externals (e.g. for benchmarking, see Chapter 8 of this report).

4.2 Evaluation by Trainers

4.2.1 Criteria / KPIs (Technical, Pedagogical, and Business)

Table 28: Questions for Survey to be Filled in by Trainers

Criteria	Question	Scale	Technical	Pedagogical	Business
Overall satisfaction	Overall, how satisfied are you with the effectiveness and efficiency of designing a training course based on CSP training materials?	7-point Likert scale	x	x	x
	Overall, how satisfied are you with the implementation of the CSP training module?	7-point Likert scale	x	x	x
Course content and structure	Based on your experience with this course, how satisfied are you as a trainer with the adaptability of the CSP training materials to fulfil the needs of your learners?	7-point Likert scale		x	
	How practically relevant do you think the training materials were for your learners in the training you offered?	7-point Likert scale			x
Learner's experience	To what extent did learners effectively engage with the course materials and activities?	7-point Likert scale		x	

	To what extent did learners demonstrate understanding and application of the concepts during the training?	7-point Likert scale		x	x
Learning platform (optional)	How satisfied are you with the performance and reliability of the platform (e.g. no errors and quick loading times) from the trainer's perspective?	7-point Likert scale	x		
	How satisfied are you with the ease of navigation of the learning platform?	7-point Likert scale	x		
	How satisfied are you with the interactivity of and engagement opportunities on the platform (e.g., quizzes, discussion forums, gamification)?	7-point Likert scale	x		
Community & interaction (optional)	How satisfied are you with the ability of the CSP training materials to facilitate interaction between you and the learners?	7-point Likert scale		x	
	How satisfied are you with the ability of the CSP training materials to facilitate interaction among participants?	7-point Likert scale		x	

Impact on students	To what extent do you think this course enhanced the knowledge and skills of students?	7-point Likert scale		x	
Recommendation	How likely are you to recommend other cybersecurity trainers to use CSP training material for their trainings?	Net Promoter Score	x	x	x
	How likely are you to host future trainings based on the CSP training materials?	Net Promoter Score		x	
	How could the CSP training materials be improved?	Open text field		x	x
	What aspects of the course delivery could be revised in future implementations?	Open text field	x	x	x
	Any further comments you like to share:	Open text field	x	x	x

4.2.2 Instruments / Tools

The evaluation of the training implementation from the trainers' perspective is also conducted using the "Evaluation Survey" feature integrated into the CSP Admin Portal. This feature allows trainers to reflect on and assess their own experience in delivering the module, focusing on aspects such as ease of use of the training materials, interaction with learners, and overall satisfaction with the training implementation process.

The trainer survey is automatically generated within the portal for each module implementation. As the survey is standardised, trainers do not need to create the survey from scratch as in the case for trainees. The survey can be found under each respective module, allowing trainers to select and complete the survey relevant to their implementation.

4.2.3 Data Collection and Analysis Process

After completing their training sessions, trainers use the CSP Admin Portal to fill out the evaluation form, reflecting on their own experience in implementing the module. The surveys are accessed through the URL or QR code provided in the admin portal, which ensured secure and direct access for each trainer.

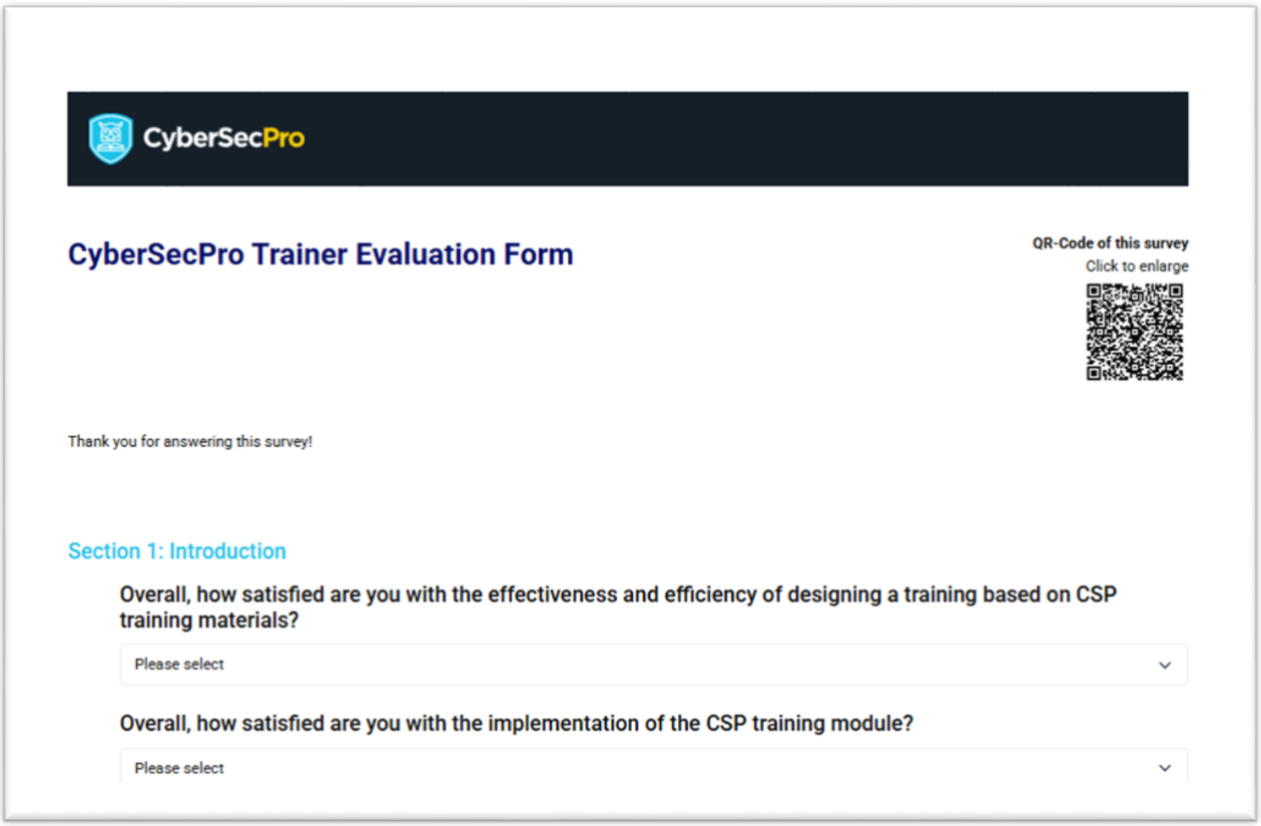

Figure 8: Screenshot of the Evaluation Form for Trainers

The completed responses are securely stored on ACEEU's server, similar to the trainee evaluations. The centralised data storage enabled streamlined data management and ensured confidentiality and accessibility for analysis.

Survey responses are visualised using bar charts generated by the CSP Admin Portal. These visual summaries provided quick insights into trainer satisfaction, challenges encountered, and suggestions for improvement.

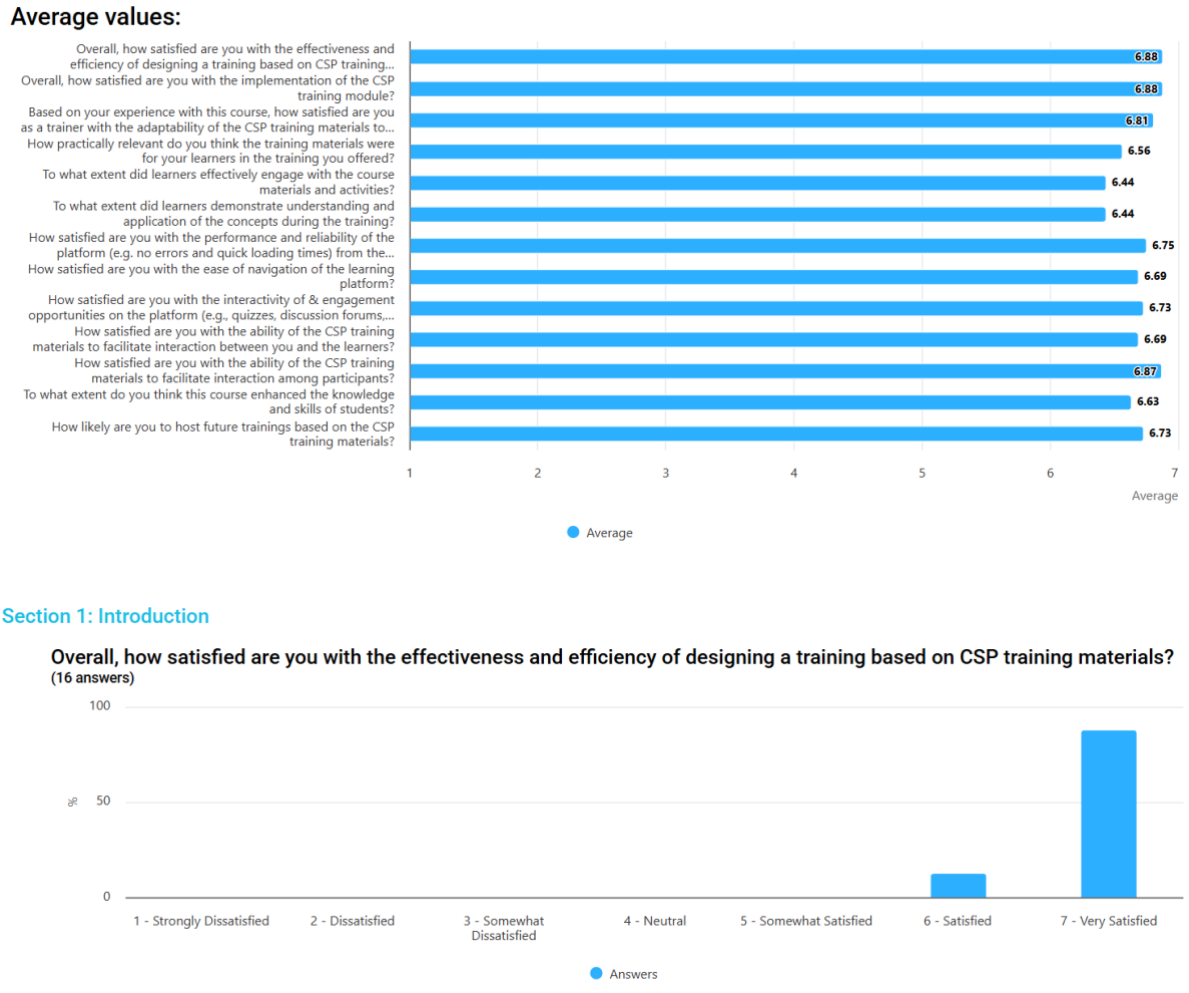

Figure 9: Visualization of Aggregated Results and Statistics from the Survey for Trainers

This approach ensured that trainers' experiences were systematically captured and analysed, contributing to the continuous improvement of module design and delivery.

5 Evaluation of MOOCs

5.1 Post-Development Implementation

To ensure the effectiveness and sustainability of the developed MOOCs of the CyberSecPro project, it is crucial to assess how well they meet defined quality criteria. As outlined in the CyberSecPro project proposal (p. 59), the quality criteria developed as part of the CyberSec4Europe project shall be taken as a basis. These criteria serve as a practical framework to evaluate and guide the implementation of MOOCs after their development. They cover essential aspects such as the qualifications of the provider, trainers, and participants; the alignment with learning outcomes and sector-specific needs; the inclusivity, ethical standards, and privacy compliance; as well as the course's practical relevance, dissemination strategy, and adaptability to market demands. Applying these criteria enables continuous improvement, recognition, and greater impact of the MOOC within the cybersecurity education landscape. The criteria were shared among WP5 members and revised based on feedback. The slightly revised criteria are presented in the next section.

5.1.1 Criteria / KPIs (Technical, Pedagogical, and Business)

Table 29: MOOC Criteria Overview

Criteria	Short description
Qualification of the provider institution	To create and offer a MOOC of high quality, the provider should have the proper qualification and experience to be able to develop, run and evaluate the MOOC professionally. The quality of the provider is also essential for the recognition of the MOOC by the community and for the recognition of credentials.
Qualifications of participants, admission criteria and inclusivity	To benefit from a MOOC, it is important that learners understand the prerequisites and trainers are aware of participants' capabilities. Non-essential prerequisites should not be used to exclude anyone, ensuring inclusivity to enhance cybersecurity competence across Europe. The acceptance process should be fair and transparent, with clear explanations provided about qualifications or reasons for non-acceptance. To ensure comprehensive inclusivity, the approach should extend beyond addressing different knowledge levels to also consider factors such as gender diversity, cultural backgrounds, and accessibility needs.
Qualification of trainers	The qualification of the trainers is fundamental to ensure a high-quality MOOC.
Course examination, credentialling and recognition	For awarding credits or certificates, examinations of the training module have to be done. Through these examinations, it is possible to (i) verify that the trainee has achieved the education goals expected (in terms of knowledge and skills required) and (ii) assure that the awarded credits or the certificate correctly reflect the level of achievement of the goals.

Course evaluation	MOOC evaluations allow trainee feedback and ratings for continuously improving the module quality, and by this, reduce the number of module dropouts.
Practical activities and quality	CyberSecPro prioritizes the level of practicality, and the MOOCs in this project should therefore maintain this level of practicality. MOOCs should be a well-rounded collection of tutorials, demonstrations, and hands-on activities that will captivate learners and emphasize their knowledge and skills.
MOOC in line to the Knowledge Areas, syllabi, and sectors identified in WP2 and WP3	MOOC designs must adhere to the predetermined Knowledge Areas in WP2 and WP3 syllabi, wherein the specified and required "learning outcomes" must be fulfilled in addition to the accepted assessment procedures and learning standards. Likewise, the content of the MOOC must be aligned with the security problems of each CSP sector (energy, health and maritime, or generic), providing specific activities and exercises, considering the technologies, protocols, and tools involved.
Meeting professional expectation	To meet professional expectations, suitable stakeholders, especially from working life and the employment side, should be involved in different MOOC phases.
Course structure and content criteria	In this section, we suggest quality criteria in terms of the MOOC content and structure. Some proposed criteria were taken from the OpenupEd suggested distinctive features (Jansen, et al., 2017), and some others were motivated by the Checklist for MOOC Accreditation in (Littlejohn, 2016) or by QRF (Stracke, et al., 2018).
Criteria for platforms and channels (for MOOC attraction and dissemination)	Important quality criteria for platforms and channels include accessibility, visibility, and criteria derived from legal requirements or conditions. Moreover, MOOCs must be self-sufficient and allow anyone to understand the procedure of each MOOC, access the content, and learn first-hand about the evaluation process. This may involve (i) initial guides to the MOOC itself, (ii) the design or development of tutorials for easy navigation, or (iii) ongoing guides with providers or trainers. In addition, it is essential to establish a suitable dissemination plan for each MOOC (or in a generalized way) to reach the corresponding networks or communities in the appropriate form. Ensuring effective dissemination enhances accessibility and engagement, allowing a broader audience to benefit from the MOOC's content and learning opportunities.
Openness	Openness is a key element of a MOOC and is important both in terms of the MOOC’s content and material, as well as in terms of being open to the learner’s needs.
Ethics & privacy	A more profound understanding of threats and risks is also needed when performing risk assessment, risk analysis and risk management. However, this knowledge could also be exploited for malicious purposes. Because of the dual nature of this knowledge, it is important to teach and enforce certain ethical principles for cybersecurity courses.

Privacy requirements, and current regulatory frameworks	As a basic requirement, the platform and the MOOC provider have to follow the legal requirements of the GDPR and EU AI Act, under specific controls.
Easy updating to enable sustainability of training and alignment with market needs	MOOCs should be designed and created so that they do not become static pieces but allow for constant modification of their online content to meet the needs of the industry and learners. The potential for updating MOOCs and, consequently, their level of sustainability, is one factor to consider.

5.1.2 Instruments / Tools

To effectively evaluate CyberSecPro's MOOCs according to the outlined quality criteria developed by the CyberSec4Europe project, various predefined instruments and tools should be utilised. These instruments are specifically designed to measure the identified KPIs comprehensively and ensure continuous improvement and alignment with the established standards for cybersecurity education.

CyberSec4Europe Evaluation Framework

The CyberSec4Europe project has developed a structured evaluation framework that provides specific criteria and indicators to measure the effectiveness of MOOCs in cybersecurity education. This framework covers pedagogical, technical, and operational aspects necessary for a comprehensive assessment.

Standardized Questionnaires

CyberSec4Europe's standardised questionnaires and surveys are tailored to evaluate:

- Participant satisfaction with course content, structure, and delivery
- Learner engagement and expectations versus outcomes
- Trainer qualifications and effectiveness.

5.1.3 Data Collection and Analysis Process

The evaluation of the MOOCs in the post-development phase will assess whether each course meets the quality standards and expectations defined within the project.

To collect relevant data for the evaluation, a dedicated evaluation survey form in MS Word format was developed and made available to MOOC providers through the CSP Admin Portal. The survey form was designed to capture self-assessment responses based on the project's established evaluation framework. MOOC providers will download the evaluation form and answer a series of structured questions that reflect the standards and expectations outlined in the project. The completed forms will be sent to the Task 5.2 leader for qualitative analysis, rating and the development of recommendations on how to improve the MOOCs.

More specifically, the following guidelines for MOOC developers have been created:

- **Download the form** from the CSP Admin Platform.
- **Work through each criterion**, inserting textual or linked evidence for how their MOOC addresses the standard.
- **Discuss internally** (e.g., with instructional designers, trainers, or quality officers) to complete uncertain sections.
- **Submit the completed form** to the WP5 evaluation team (and store it for internal records if used as a development tool).
- Use feedback from the evaluation team to **revise the MOOC** or to **benchmark it** against other courses in the CyberSecPro portfolio.

5.1.4 Feedback and Revision

The feedback and revision processes were conducted systematically to ensure the robustness and validity of the evaluation criteria and instruments developed. Initially, the criteria and assessment tools were reviewed by the Work Package 5 (WP5) leader. After incorporating the initial feedback from the WP5 leader, the refined version was circulated among all WP5 members for further evaluation and comments.

WP5 members provided detailed feedback, highlighting strengths and areas for improvement.

Based on this collective input, revisions and refinements were made to enhance the clarity, effectiveness, and practicality of the evaluation framework. This collaborative approach facilitated a comprehensive and inclusive revision process, significantly improving the final evaluation criteria and instruments.

Key points raised included:

1. Suggestions for new criteria and corresponding descriptions related to practical activity and quality, as well as better alignment of sector focus across WP2 and WP3 (Energy, Health, Maritime, General).
2. A recommendation to clarify and consistently distinguish between the terms “Providers” and “Trainers.”
3. Feedback on the Self-Evaluation Form, specifically regarding how it reflects the proposed criteria.

5.2 Pre-Development Implementation

The evaluation criteria derived from the CyberSec4Europe framework will also serve as a foundational reference for guiding and assessing the development of CyberSecPro MOOCs during the development process. Thus, this process complements the post-development usage as explained in the previous section.

The framework will function as a structured quality assurance checklist, supporting MOOC providers throughout the development process. Rather than being used only after course development, the criteria will be applied from the early stages onward—as a guidance tool during planning and design, and as a benchmark for continuous alignment with the project’s learning objectives and quality standards. Providers are expected to use a standardised Microsoft Word-based self-assessment form to reflect on and document their progress. This form will help ensure that key elements such as course structure, trainer qualifications, ethical considerations, and platform usability are addressed systematically.

By employing a unified set of evaluation criteria, the project will promote consistency and comparability across all MOOCs, regardless of content area or format. The structured use of the criteria will also facilitate early identification of potential gaps, enabling timely improvements before courses are finalized and published.

Through this forward-looking approach, the CyberSecPro project will ensure that each MOOC is developed in line with the overarching goals of high-quality cybersecurity education and adheres to the strategic framework defined in earlier work packages. In this way, the evaluation criteria will not only assess completeness and quality but also actively support development and alignment throughout the course creation process.

6 Evaluation Planning / Logistics

6.1 Recommendation for Quantitative Data Analysis

Quantitative data analysis in CyberSecPro primarily stems from structured feedback instruments such as post-training surveys, MOOC evaluation questionnaires, and platform-generated analytics (e.g. completion rates, engagement statistics, satisfaction scores). The analysis aims to ensure comparability across training modules and cohorts while enabling evidence-based decision-making. The following key practices are recommended:

- **Descriptive Statistics**: Calculate mean, median, and standard deviation for core metrics such as trainee satisfaction, trainer recommendation rate (e.g. Net Promoter Score), and perceived usefulness.
- **Cross-Tabulation**: Use demographic variables (e.g. country, professional background) to identify trends across learner groups.
- **Trend Analysis**: Compare outcomes over time and between modules to identify consistent patterns or deviations.
- **Visualisation**: Present key data in dashboards using bar charts, histograms, and heatmaps for clear, communicable insights.
- **Correlation Analysis**: Explore relationships between engagement levels and satisfaction or learning outcomes, particularly where enough sample size allows.

Quantitative results should be aggregated in a way that respects participant anonymity and complies with GDPR requirements. Only de-identified, summarised data shall be used for benchmarking and dissemination purpose.

Thresholds

To guide interpretation, CyberSecPro recommends the use of threshold values to classify results into actionable categories. The following indicative thresholds can be applied:

Table 30: Recommended Thresholds

Metric	Excellent	Satisfactory	Needs Improvement
Overall Satisfaction (avg. ≥ 1–7)	≥ 6.0	4.5–5.9	< 4.5
Net Promoter Score (NPS)	> 30	0–30	< 0
Content Relevance (avg. score)	≥ 6.0	4.5–5.9	< 4.5
Completion Rate (in MOOCs)	≥ 50%	30–49%	< 30%

Thresholds should be adapted based on training type (e.g. MOOCs vs. live workshops), module complexity, and learner characteristics. They provide a reference point for identifying outliers and prioritising areas for course improvement or follow-up.

6.2 Recommendation for Qualitative Data Analysis

Qualitative data complements quantitative insights by capturing nuanced perspectives on course content, delivery, and learner experience. In this respect, the suggested evaluation methodology primarily features open-text survey questions for trainee and trainer reflections.

To ensure consistency and analytical depth, the following approach is recommended:

- **Thematic Coding**: Employ open and axial coding to identify recurring themes and sub-themes related to learning satisfaction, technical usability, pedagogical quality, and professional relevance.
- **Matrix Analysis**: Cross-compare themes across different respondent groups (e.g., trainees vs. trainers) or modules.
- **Sentiment Analysis** (optional): Use software tools or manual coding to classify feedback as positive, negative, or neutral (might be challenging due to the short answers).
- **Quotations**: Select representative quotes to illustrate key findings in evaluation reports.
- **Traceability**: Link qualitative insights to specific questions or learning objectives for targeted refinement of the course content or delivery.

Qualitative results should be anonymised and used primarily to explain patterns found in the quantitative data or to identify needs not captured by structured instruments.

6.3 Triangulation and Mixed-Method Insights

To strengthen the validity of findings and deepen interpretation, triangulation of data sources is encouraged:

- **Compare quantitative survey scores with qualitative comments** to verify consistency.
- **Cross-reference platform analytics (e.g. dropout points) with learner feedback** to explain behavioural patterns.
- **Use trainer interviews or course logs** to contextualise learner responses and course challenges.

This mixed-method approach ensures that decisions about course revision, improvement, or scaling (e.g. CSP exploitation as part of Task 6.3) are grounded in a rich, evidence-informed understanding of training effectiveness.

6.4 Timing

The evaluation instrument has been made available since April. Trainers are recommend inviting students from previous training sessions to complete the survey if the training has been completed in the past 2 months. The evaluation can be conducted from the date of availability through the end of the project and may also be used beyond the project's duration. To maximize response rates, we suggest administering the survey during class sessions.

6.5 Roles and Responsibilities

The following table outlines specific tasks and duties assigned to CSP partners and stakeholders, ensuring coordinated efforts, clear accountability, and efficient execution of evaluation activities.

Table 31: Roles and Responsibilities

Partner/Stakeholder	Role and Responsibilities
ACEEU	Provision and timely updates of evaluation instruments, particularly in case of identified errors or required adjustments.
COFAC	Task leader of Task 5.2, responsible for coordinating comprehensive data collection and analysis.
Trainers	Creation, dissemination, and completion of training-specific surveys to gather feedback and assess training effectiveness.
GUF	Encouraging trainers to input details of module implementation into the administrative portal for comprehensive tracking.
Training Material Developers	Reviewing evaluation outcomes and updating training materials to maintain ongoing quality and relevance.

7 Usage of CyberSecPro Evaluation Data for Benchmarking

7.1 Internal Benchmarking

To better understand what types of training lead to higher student satisfaction and engagement, T5.1 provides ideas for an internal benchmarking approach. This process aims to compare and analyse the different dimensions of course implementation across the consortium. By examining patterns across formats, sectors, and providers, the benchmarking exercise will support continuous improvement and help identify which elements contribute most effectively to learner satisfaction and impact.

The benchmarking will consider a wide range of variables, including:

1. **Training level**: Differentiating between basic and advanced courses.
2. **Sector focus**: Comparing courses targeting specific sectors such as health, maritime, and energy.
3. **Provider-specific comparison**: Benchmarking courses delivered within the same institution or provider.
4. **Delivery mode**: Comparing virtual, hybrid, and in-person training formats.
5. **Module type**: Comparing multiple module delivery types including courses, workshops, seminars, cybersecurity exercises, summer schools, and hackathons.
6. **Modules**: Comparing performance across CP001 to CP012.
7. **Knowledge areas**: Benchmarking by the cybersecurity knowledge domains the modules address.
8. **Capability categories**: Benchmarking by the types of skills and competencies targeted (e.g., technical, soft, or operational).
9. **Provider type**: Comparing training run by universities, companies, or through joint efforts.
10. **Assignment inclusion**: Analysing whether modules that include assignments yield higher satisfaction.
11. **Course language**: Assessing whether language affects learner satisfaction.
12. **Trainer profile**: Comparing the involvement of external trainers and industry experts.
13. **ECTS allocation**: Comparing learner satisfaction between courses that offer ECTS credits and those that do not.
14. **Certification**: Comparing learner satisfaction between courses that offer a certificate of attendance and those that do not.
15. **DCM and other platforms**: Comparing modules delivered through the DCM and other tools.
16. **Course duration**: Comparing module by course length.

This multidimensional approach will provide the project team with insights into which combinations of course features are most valued by participants, ultimately informing the refinement of future training offers.

7.2 External Benchmarking

In addition to internal performance comparisons, T5.1 also outlines a possible direction for external benchmarking, recommending that selected evaluation data and training metadata be shared publicly to support comparison and learning beyond the project. The goal is to allow other organisations, universities, training providers, and policy actors to compare their own cybersecurity training offers against CyberSecPro's results and standards.

To ensure full compliance with data protection regulations, all shared data will be fully anonymised. No personally identifiable information will be included, and no individual respondent — whether learner, trainer, or evaluator — will be identifiable in any published data. Aggregated and de-identified results will be used to preserve privacy while still enabling meaningful insights for external stakeholders.

By sharing this data openly, the project supports transparency, collaboration, and improvement across the broader cybersecurity education landscape. External stakeholders will be able to benchmark against various indicators such as training type, delivery mode, sector focus, learning outcomes, and participant satisfaction.

To support this, Task 5.2 shall:

- Provide anonymised datasets summarising course characteristics and evaluation results (e.g. as CSV export)
- Ensure documentation of training modules (e.g. level, length, mode, ECTS, trainer type) is accessible
- Highlight key benchmarks and good practices derived from internal analysis
- Encourage adaptation of the evaluation instruments and methodology by other providers.

This openness positions CyberSecPro as a reference point for quality and effectiveness in cybersecurity training and fosters a shared culture of evidence-based improvement in the sector.

8 Conclusion

8.1 Summary

This report, D5.1, outlines a comprehensive, research-based evaluation methodology for the CyberSecPro project, designed to assess the effectiveness and impact of its cybersecurity training programs. The framework is grounded in international standards and integrates best practices from initiatives like CyberSec4Europe and BIBLIO. Its primary purpose is to measure performance, usability, and quality, particularly for the MOOCs developed in the project. The methodology is purpose-driven, focusing on experiential feedback rather than purely technical skills. It employs a mix of quantitative and qualitative tools to gather data from multiple perspectives. Evaluation strategies are detailed for:

- **Trainees**: Assessing overall satisfaction, the quality and relevance of course content, instructor effectiveness, and the learning platform's usability. Data is collected via a digital survey tool in the CSP Admin Portal.
- **Trainers**: Evaluating their experience with the provided materials, including adaptability and the ability to facilitate learner engagement. This is also conducted through a survey feature in the CSP Admin Portal.
- **MOOCs**: A post-development evaluation ensures courses meet quality criteria derived from the CyberSec4Europe framework. This involves a self-assessment by MOOC providers using a dedicated survey.

The collected data supports both internal and external benchmarking. Internally, it allows for comparison across different course formats, sectors, and providers to identify best practices. Externally, the project plans to share anonymised data to help other organisations benchmark their own training programs, fostering transparency and improvement across the cybersecurity education landscape. The methodology and its instruments are designed to be reusable beyond the project's lifetime.

8.2 Contributions

The work carried out in Task 5.1 will generate significant added value across multiple areas of the CyberSecPro project. By establishing a robust evaluation methodology and set of instruments, this task provides a foundation for both internal improvements and broader project alignment. The following outlines how the outputs of Task 5.1 and this Deliverable 5.1 will contribute to other work packages, strengthening the overall coherence, impact, and sustainability of the project.

Key Contributions to Other Work Packages

- **WP3 Training Implementation**

  Evaluation results will inform the revision and refinement of training content developed under this work package.

- **WP5 Evaluation (Task 5.2):**

  The methodology and instruments designed in Task 5.1 will serve as the basis for data collection and analysis activities in Task 5.2.

- **WP6 Dissemination and Exploitation:**

- **Task 6.2:** Insights from the evaluation will support the design of targeted dissemination strategies.
- **Task 6.4:** Findings will also inform the exploitation planning by identifying effective practices and impactful training formats.

References

1. Chan, V. K. (2023). Evaluating Popular MOOC Platforms by Generative Artificial Intelligence (AI) Robots: How Consistent Are the Robots? International Association for Development of the Information Society.
3. Bali, M. (2014). MOOC pedagogy: Gleaning good practice from existing MOOCs. Journal of Online Learning and Teaching, 10(1), 44.
4. Douglas et al. (2019). Meaningful learner information for MOOC instructors examined through a contextualized evaluation framework. International Review of Research in Open and Distributed Learning, 20(1).
5. Sebbaq, H., & El Faddouli, N. E. (2024). Towards quality assurance in MOOCs: a comprehensive review and micro-level framework. The International Review of Research in Open and Distributed Learning, 25(1), 1-23.
6. Stephens, M., & Jones, K. M. (2014). MOOCs as LIS professional development platforms: Evaluating and refining SJSU's first not-for-credit MOOC. Journal of Education for Library and Information Science, 345-361.
7. Aloizou, V. (2018). Quality assurance methods assessing instructional design and active learning pedagogies in MOOCs: an evaluative case study (master's thesis, Πανεπιστήμιο Πειραιώς).
8. Tzeng et al. (2022). MOOC evaluation system based on deep learning. International Review of Research in Open and Distributed Learning, 23(1), 21-40.
9. Duan, T., & Wu, B. (2023). The Student Self-Assessment Paradigm in MOOC: An Example in Chinese Higher Education. Comunicar: Media Education Research Journal, 31(75), 111-123.
10. Ferreira et al. (2022). Quality criteria in MOOC: Comparative and proposed indicators. Plos one, 17(12), e0278519.
11. Poce et al. (2019). Establishing a MOOC Quality Assurance Framework--A Case Study. Open Praxis, 11(4), 451-460.
12. Sabjan et al. (2021). MOOC quality design criteria for programming and non-programming students. Asian Journal of University Education, 16(4), 61-70.
13. Shah et al. (2023). Is My MOOC Learner-Centric? A Framework for Formative Evaluation of MOOC Pedagogy. International Review of Research in Open and Distributed Learning, 24(2), 138-161.
14. Stracke et al. (2018). Fostering Quality in MOOCs: a European Approach. In European Conference on E-Learning (ECEL 2018) (pp. 533-538). ACPIL.
15. Yılmaz, A. B., Ünal, M., & Çakır, H. (2017). Evaluating MOOCs according to instructional design principles. Journal of Learning and Teaching in Digital Age, 2(2), 26-35.
16. Gatomati, F. (2021). BIBLIO Massive Open Online Course (MOOC) Evaluation Report (WP4 – Deliverable 4.2). BIBLIO Project Consortium.
17. Fischer-Hübner, S., Beckerle, M., Lluch Lafuente, A., Ruiz Martínez, A., Saharinen, K., Skarmeta, A., & Sterlini, P. (2020). Quality criteria for cyber security moocs. In Information Security Education. Information Security in Action: 13th IFIP WG 11.8 World Conference, WISE 13, Maribor, Slovenia, September 21–23, 2020, Proceedings 13 (pp. 46-60). Springer International Publishing.
18. Iniesto, F. (2021). Models and Guidelines for Assessment and Recognition of MOOCs and microcredentials. EMC-LM Project deliverable 4.2.
19. Ferrari, C. M., Pennati, C., & Tammets, K. (2014). D4.2 Evaluation Methodology (Learning Data Collection and Evaluation). European Multiple MOOC Aggregator (EMMA) Project. Ipsos, Tallinn University.
20. Cirlan, E., & Loukkola, T. (2020). European project MICROBOL: Micro-credentials linked to the Bologna Key Commitments. Brüsszel, Európai Egyetemek Szövetsége.

21. SCORE2020 Project. (2016). OpenupEd quality assurance checklists: Self-assessment for MOOC providers. OpenupEd & EADTU.
22. Littlejohn, A. (2016). Guidelines for Quality Assurance and Accreditation of MOOCs.
23. Jansen, D., Rosewell, J., & Kear, K. (2017). Quality frameworks for MOOCs. Open education: from OERs to MOOCs, 261-281.
24. Scriven, M. (2007). Key evaluation checklist (KEC). *Retrieved April*, *15*, 2007.
25. Davidson, D. (2006). *The Essential Davidson*. Oxford University Press.
26. Gibbs, G. (2010) Dimensions of Quality. The Higher Education Academy. www.heacademy.ac.uk
27. Askeroth, J. H., & Richardson, J. C. (2019). Instructor perceptions of quality learning in MOOCs they teach. *Online Learning*, *23*(4), 135-159. https://doi.org/10.24059/olj.v23i4.2043.
28. Bonk, C. J., Zhu, M., Kim, M., Xu, S., Sabir, N., & Sari, A. R. (2018). Pushing toward a more personalized MOOC: Exploring instructor selected activities, resources, and technologies for MOOC design and implementation. The International Review of Research in Open and Distributed Learning, 19(4), Article 4. https://doi.org/10.19173/irrodl.v19i4.3439.
29. Ray, S. (2019, February). A quick review of machine learning algorithms. In 2019 International conference on machine learning, big data, cloud and parallel computing (COMITCon; pp. 35-IEEE. https://doi.org/10.1109/COMITCon.2019.8862451).

Annex A: Questions for Trainers and the Guiding Reference

Criteria	Question		Guiding Literature/Reference
Overall Satisfaction	How would you rate your overall satisfaction with the training module?		CyberSecPro
Course content and structure	How satisfied are you with …	overall quality of instructional materials?	CyberSec4Europe Approach; Chan, 2021; Shah et al., 2023; Fereira et al., 2022; Stracke et al., 2018;
		the clarity of instructional materials?	
		the practical relevance of the content (e.g. needed practical skills, real-world scenarios, professional contexts, and industry standards)?	BIBLIO Framework; Alturkistani et al., 2020; ENQA Framework
		the alignment of course design and content with the intended learning objectives?	Shah et al., 2023; BIBLIO Framework; Stephen and Jones, 2024
Instructor	How satisfied are you with …	the instructor's knowledge and competence brought into the training module?	CyberSec4Europe Approach
		the instructor's responsiveness and support?	ENQA Framework; Chan, 2023; Bali, 2014
		the instructor's teaching approach?	Tzeng et al., 2022; Chan, 2021; Jansen et al., 2017; Fereira et al., 2022; Alturkistani et al., 2020;

Learning Platform	How satisfied are you with …	the accessibility of the learning platform?	OpenupEd Framework; ENQA Framework;
		the ease of navigation of the learning platform?	
		the performance and reliability of the platform (e.g. no errors and quick loading times)?	BIBLIO Framework; Chan, 2014; OpenupEd
		the visual appeal of the platform?	
		the interactivity of & engagement opportunities on the platform (e.g., quizzes, discussion forums, gamification)?	ENQA Framework
Community/ Interaction	How satisfied are you with …	the interactions facilitated between learners and external actors (e.g. invited experts)	ENQA Framework; Bali, 2014
		the interactions facilitated between learners	Yimlaz et al., 2017; Chan, 2023; Bali, 2014
Evaluation/ Recognition	How satisfied are you with …	the transparency of the examination process?	CyberSec4Europe Approach; EMC-LC Framework
		the fairness of the examination process?	CyberSec4Europe Approach
		the value the (attendance) certificate provides in your professional or academic field?	Littlejohn, A., 2016
Impact on students	How relevant are the skills and knowledge gained to your current or desired job role?		Bali, 2014
	To what extent did this course enhance your knowledge and skills?		Scriven, 2015; and Davidson, 2005

	How likely are you to further explore the topic of the module (e.g. through self-learning or another course)?	Duan and Wu (2023)
Recommendation	How likely are you to recommend this learning experience to someone looking to improve skills in the cybersecurity field?	CyberSecPro
	How could the overall learning experience be enhanced?	CyberSecPro
	Any further comments you like to share?	CyberSecPro

Annex B: Quality Criteria for Evaluating MOOCs

These criteria, based on results from the CyberSec4Europe[1] project, offer a valuable framework for evaluating or designing training modules through Massive Open Online Courses (MOOCs). As specified in the CyberSecPro[2] Grant Agreement, the criteria developed in the CyberSec4Europe shall be applied for evaluating CyberSecPro MOOCs.

We suggest using the criteria in two ways:

1. Those who develop CyberSecPro MOOCs shall take into account these criteria in their development process to ensure **quality, accessibility, and effectiveness** of their MOOCs.
2. Once the CyberSecPro MOOCs are developed, the criteria shall be used by the CyberSecPro consortium (Task 5.2) to evaluate the developed MOOCs, based on evidence provided by the MOOC developers.

Please note that for reasons of readability, the following criteria are referring to "providers" as a catch-all terms that includes those that develop, run and evaluate MOOCs. It might be the case that stakeholders are only involved in the development, implementation and/or evaluation.

Criteria	Short description
Qualification of the provider institution	To create and offer a MOOC of high quality, the provider should have the proper qualification and experience to be able to develop, run and evaluate the MOOC in a professional manner. The quality of the provider is also essential for the recognition of the MOOC by the community and for the recognition of credentials.
Qualifications of participants, admission criteria and inclusivity	To benefit from a MOOC, it is important that learners understand the prerequisites and trainers are aware of participants' capabilities. Non-essential prerequisites should not be used to exclude anyone, ensuring inclusivity to enhance cybersecurity competence across Europe. The acceptance process should be fair and transparent, with clear explanations provided about qualifications or reasons for non-acceptance. To ensure comprehensive inclusivity, the approach should extend beyond addressing different knowledge levels to also consider factors such as gender diversity, cultural backgrounds, and accessibility needs.

[1] CyberSecd4Europe, https://cybersec4europe.eu

[2] CyberSecPro, https://www.cybersecpro-project.eu

Qualification of trainers	The qualification of the trainers is fundamental to ensure a high-quality MOOC.
Course examination, credentialization and recognition	For awarding credits or certificates, examinations of the training module have to be done. Through these examinations, it is possible to (i) verify that the trainee has achieved the education goals expected (in terms of knowledge and skills required) and (ii) assure that the awarded credits or the certificate correctly reflects the quality with that the goals were achieved.
Course evaluation	MOOC evaluations allow trainee (i) feedback and ratings for continuously improving the module quality, and by this, (ii) reduce the number of module dropouts.
Practical activities and quality	CyberSecPro prioritizes the level of practicality, and the MOOCs in this project should therefore maintain this level of practicality. Learners should find MOOCs a rich showcase of hands-on activities, demonstrations and tutorials to engage learners and emphasize skills and knowledge.
MOOC in line to the Knowledge Areas, syllabi, and sectors identified in WP2 and WP3	The design of MOOCs must be in line with the predefined Knowledge Areas in WP2 and syllabi in WP3, where the expected and stated "learning outcomes" must be met, as well as the established assessment methods and learning criteria. Likewise, the content of the MOOC must be aligned with the security problems of each CSP sector (energy, health and maritime, or generic), providing specific activities and exercises, considering the technologies, protocols and tools involved.
Meeting professional expectation	For meeting professional expectations, suitable stakeholders, especially from working life and the employment side, should be involved in different MOOC phases.
Course structure and content criteria	In this section, we suggest quality criteria in terms of the MOOC content and structure. Some of the proposed criteria were taken from the OpenupEd suggested distinctive features (Jansen, et al., 2017), and some others were motivated by the Checklist for MOOC Accreditation in (Littlejohn, 2016) or by QRF (Stracke, et al., 2018).
Criteria for platforms and channels (for MOOC attraction and dissemination)	Important quality criteria for platforms and channels include accessibility, visibility, and criteria derived from legal requirements or conditions. Moreover, MOOCs must be self-sufficient and allow anyone to understand the procedure of each MOOC, access the content, and learn first-hand about the evaluation process. This may involve (i) initial guides to the MOOC itself, (ii) the design or development of tutorials for

	easy navigation, or (iii) ongoing guides with providers or trainers. In addition, it is essential to establish a suitable dissemination plan for each MOOC (or in a generalized way) to reach the corresponding networks or communities in the appropriate form. Ensuring effective dissemination enhances accessibility and engagement, allowing a broader audience to benefit from the MOOC's content and learning opportunities.
Openness	Openness is a key element of a MOOC. Openness is important both in terms of the MOOC content and material, and in terms of being open to the learner's needs.
Ethics and Privacy	A deeper understanding of threats and risks is also needed when performing risk assessment, risk analysis and risk management. However, this knowledge could also be exploited for malicious purposes. Because of this dual nature of this knowledge, it is important to teach and enforce certain ethical principles for cybersecurity courses.
Privacy requirements, and current regulatory frameworks	As a basic requirement, the platform and the MOOC provider have to follow the legal requirements of the GDPR and EU IA Act, under specific controls.
Easy updating to enable sustainability of training and alignment with market needs	MOOCs should be designed and created so that they do not become static pieces but allow for constant modification of their online content to the needs of the industry. Therefore, one aspect to evaluate is the degree of updating that MOOCs could have, and therefore, their degree of sustainability.

Self-evaluation form for MOOC providers

Quality of the Provider

QC 1. The provider should be recognised by the relevant stakeholders in the cybersecurity community as having expertise in the area. This could be either by academic recognition or long experience within the area or related areas or other criteria that the stakeholders may find relevant.

[Please insert your evidence here]

Quality of Participations and Admission Criteria

QC 2. The MOOC should include only the essential requirements needed for participants to follow and understand the course content.

[Please insert your evidence here]

QC 3 The MOOC requirements should be clearly explained, including the reasons for their necessity. Participants should be provided with guidance on how to meet these requirements, such as recommended courses or learning materials.

[Please insert your evidence here]

QC 4. The MOOC must be accessible and accept participants in a fair and transparent manner and should state the acceptance process and, if the number of participants is limited, the criteria and process for selection of participants.

[Please insert your evidence here]

Qualifications of the Trainers

QC 5. Trainers must possess an academic degree or relevant qualifications and experience in the teaching area, along with pedagogical training acquired through prior teaching experience, completed courses on higher education pedagogy, or other equivalent means.

[Please insert your evidence here]

Course Examination, Credentialisation and Recognition

QC 6. The MOOC should be recognised as a valid credit-awarding training module within the European Credit Transfer System (ECTS).

[Please insert your evidence here]

QC 7. Examination content, especially in terms of course learning outcomes to be demonstrated in the exam, and the assessment form and assessment criteria should be clear and transparent.

[Please insert your evidence here]

QC 8. Assessment methods must be aligned with the learning objectives and be measured by valid means (JRC Report, 2016).

[Please insert your evidence here]

QC 9. The examination process must be fair, follow legal procedures, take appropriate measure to correctly identify the participants to be examined and thus minimize the possibility of lacking of authorship or cheating – independently of whether the course examination takes place online or at a physical location.

[Please insert your evidence here]

QC 10. The time frame, in which the course needs to be finished in order to receive the credits or credentials, must be clearly stated. Also, the expected course workload including efforts for course assignments or laboratory work, etc. and deadlines for completion, need to be made clear and transparent.

[Please insert your evidence here]

QC 11. Obtaining a course certificate should not just be based on payment of fees, but on an actual verification that the participant fulfilled the learning objectives.

[Please insert your evidence here]

QC 12. Course certificates should be designed to enable recognition of the educational achievements in the professional or life-long/blended learning context.

[Please insert your evidence here]

Course Evaluation

QC 13. The trainers and/or providers should review the MOOC and its content periodically, and in line to the Knowledge Areas identified in WP2 and the syllabi proposed in WP3. Likewise, the content must be current and meet learning objectives to be in line with the needs of the market (WP2-WP3). The period of this review should be appropriate to the speed of development and changes in the area of the module scope.

[Please insert your evidence here]

QC 14. There should be means in place for the participants to continuously, or at least periodically, evaluate the MOOC and to provide feedback. Suitable course-specific feedback channels or discussion forums should be used for receiving continuous participant's feedback. If the evaluation is done periodically, it should be conducted at least once: when a participant finishes the course.

[Please insert your evidence here]

QC 15. Means for conducting anonymous online course evaluations by the participants should be offered.

[Please insert your evidence here]

QC 16. An evaluation review process should be in place that should involve relevant stakeholders (such as MOOC design team, trainers, director of studies). The relevant stakeholders should utilise available learning analytics, document the findings, and provides recommendations to improve the MOOC.

[Please insert your evidence here]

QC 17. Summaries of evaluations and measures taken in response to the evaluation to remedy shortcomings or improve the MOOC should be easily accessible and published on the same channel/ platform as the MOOC.

[Please insert your evidence here]

QC 18. The implementation, effect, and changes of proposed improvements should achieve their expected impact. Relevant stakeholders should evaluate this.

[Please insert your evidence here]

Meeting Professional Expectation

QC 19. In the early development phases of the course, an analysis should be done identifying stakeholders and their expectations.

[Please insert your evidence here]

QC 20. Different relevant stakeholder representatives should be involved in the design, implementation, realization, and in periodic reviews of the MOOC. This means that their involvements can be in the form of advisors, guest professors or external evaluators.

[Please insert your evidence here]

Course Structure and Content Criteria

QC 21. There have to be specific learning outcomes defined for each MOOC and course examination and quizzes should be aligned with the learning outcomes. The evaluation of participants should test the alignment.

[Please insert your evidence here]

QC 22. The MOOC should provide an overview, which prominently and in sufficient detail publishes the purpose and structure of the MOOC, the main content, format (the teaching methods used and learning activities required of students, assessment methods and criteria), reference literature, language, the learning outcomes including knowledge and skills (memorize, understand, apply, analyse, evaluate, or create) as prerequisites and knowledge (theoretical), skills to be acquired (practical, methodological, or applied), and instructor's profiles. All this means that the material to be produced must also be in line to the criteria established in WP3 and its corresponding syllabi and sector. Please, refer to D3.3, D3.4 and D3.5.

[Please insert your evidence here]

QC 23. The content of the MOOC should be such the learning outcomes can be fulfilled. There must be alignment between the teaching methods, learning activities, assessment methods and the learning outcomes – please refer to WP3 to be in line to the mentioned and corresponding syllabi.

[Please insert your evidence here]

QC 24. The MOOC should cater for different learning styles and strategies to reach the leaning outcomes and address the diversity and inclusivity.

[Please insert your evidence here]

QC 25. MOOCs should follow a Learner-centred approach, as defined by OpenupEd: They should "aid students to construct their own learning styles from a rich environment, and to share and communicate it with others; they should not simply focus on the transmission of content knowledge to the student" (Jansen et al., 2017).

[Please insert your evidence here]

QC 26. MOOCs should enable independent learning and should, as suggested by OpenupEd, provide high quality materials to enable an independent learner to progress through self-study (Jansen et al., 2017).

[Please insert your evidence here]

QC 27. MOOCs should provide "media-supported interactions", as proposed by OpenupEd: "Course materials should make best use of online affordances (interactivity, communication, and collaboration) as well as rich media (video and audio) to engage participants with their learning" (Jansen et al., 2017).

[Please insert your evidence here]

QC 28. As suggested by OpenupEd, there should be a consistent focus in terms of the production and presentation of the MOOC (Jansen et al., 2017). This also means that all course material is appropriately cited, and copyright clearance has been obtained if necessary. Web links used are relevant and functional.

[Please insert your evidence here]

QC 29. The course material's design should be made accessible to different audience and should meet the requirements of EU Directive 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies. In particular, videos should include subtitles or scribes of the voice recording in English.

[Please insert your evidence here]

QC 30. The MOOC should include instructions that clarify how participants can obtain technical support.

[Please insert your evidence here]

Criteria for Platforms and Channels

QC 31. Privacy and security concerns should be addressed when selecting channels and platforms for learning content. Particularly, GDPR compliant platforms, preferably located in Europe, must be used, and platform should be hosted by trustworthy third parties or hosted directly by the MOOC provider. In case of AI usage, the EU AI Act should be followed.

[Please insert your evidence here]

QC 32. It should be easily possible for a broad audience to find and use the platforms used for the MOOC.

[Please insert your evidence here]

QC 33. The platform should provide the functionality to comply with the EU Directive 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies.

[Please insert your evidence here]

Openness and Dissemination

QC 34. The MOOC should enforce openness to learners by adapting to their needs, as suggested by OpenupEd (Jansen et al., 2017). It should possibly try to enable the freedom to study any time, place and pace of choice.

[Please insert your evidence here]

QC 35. MOOCs should enforce digital openness: They should "be freely available online but in addition apply open licensing so that material and data can be reused, remixed, reworked and redistributed (e.g. using CC-BY-SA or similar)" (Jansen et al., 2017).

[Please insert your evidence here]

QC 36. There should be suitable policies for defining any restrictions to digital openness and/or openness to learners for ethical or security reasons.

[Please insert your evidence here]

QC 37. The MOOC should use open educational literature and resources.

[Please insert your evidence here]

Ethics and Privacy

QC 38. There should be a code of conduct for course participants stating expected and unacceptable use of knowledge, tools and facilities under ethical codes and procedures, both during and after the course.

[Please insert your evidence here]

QC 39. The MOOC should avoid going into detailed aspects of attack methodology and techniques for finding vulnerabilities, if it is not necessary for achieving the learning outcomes of the MOOC. This should especially be considered in totally open courses.

[Please insert your evidence here]

QC 40. MOOC participants should be made aware of the ethical and privacy aspects of security monitoring and surveillance technologies, and countermeasures.

[Please insert your evidence here]

QC 41. MOOC participants should be made aware of the proper way of handling and reporting vulnerabilities that they might find.

[Please insert your evidence here]

Privacy Requirements

QC 42. Privacy Policy (Art. 29 GDPR): There must be a clear policy statement, both from the platform and the MOOC owner, which includes information about the data controller of the different types of personal data, what personal data is processed by whom and for what purposes. Particularly the extent, purpose and consequences of participants profiling needs to be made transparent and should require the participant's explicit consent.

[Please insert your evidence here]

QC 43. The platform and MOOC provider must assure that the participants can exercise their data subject rights pursuant to the GDPR, preferably also by electronic means.

[Please insert your evidence here]

QC 44. If personal data is used for marketing purposes, there should be an opt-in option rather than an opt-out option for that purpose.

[Please insert your evidence here]

QC 45. There must be a valid and clear data processor agreement between the "owner" of the MOOC (in the role of the data controller) and the platform (in the role of the data processor) (Art. 28 GDPR).

[Please insert your evidence here]

QC 46. If a privacy "unfriendly" channel is used, the participants of the MOOC should be given a more privacy friendly alternative.

[Please insert your evidence here]

QC 47. The platform and course instances storing personal data about the participants must be secured by appropriate security controls and should be designed by the Data Protection by Design and Default principle (Art. 25 GDPR), aligned with the consortium agreement regarding the storing period beyond the project.

[Please insert your evidence here]

Easy updating to enable sustainability of training and alignment with market needs

QC 48: Is there a system in place to regularly update the MOOC content to keep it aligned with industry needs?

[Please insert your evidence here]

QC 49: Does the MOOC allow for easy modifications to ensure its long-term relevance and sustainability?

[Please insert your evidence here]

Evaluation Form for MOOCs

Each section from the self-evaluation form presented above shall be evaluated using the following assessment scale:

[ ] Fulfilled

[ ] Partially fulfilled

[ ] Not fulfilled

References

Jansen, D., Rosewell, J., & Kear, K. (2017). Quality frameworks for MOOCs. Open education: from OERs to MOOCs, 261-281.

Stracke, C., Sgouropoulou, C., Vassiliadis, B., Kameas, A., Teixeira, A., & Pinto, M. D. C. T. (2018). Fostering quality in moocs: A european approach. In European Conference on E-Learning (ECEL 2018) (pp. 533-538). ACPIL.

Littlejohn, A. (2016). Guidelines for Quality Assurance and Accreditation of MOOCs.

Joint Research Centre. (2016). JRC annual report 2016. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC106440