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

Project start: 2022-12-01
Project duration: 39 months

CyberSecPro

D6.4
Grouped Exploitation Plans

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

Related WP	WP6	Dissemination Level	PU
Lead Participant	ACEEU	Lead Author	Lina Landinez, Thorsten Kliewe (ACEEU)
Contributing Participants	All Partners	Related Deliverables	D6.1, D6.3, D6.5

Abstract: This deliverable presents the group exploitation plans of the CyberSecPro project, documenting how the consortium translates its key exploitable results (KERs) into coordinated, multi-partner pathways for post-project continuation and impact. Building on a structured methodology from KERs to exploitation pathways to action-oriented plans, the report consolidates group-level exploitation options across education, open access/public impact, industry and professional training, community building, and commercialisation. It then develops detailed group exploitation plans for three priority pathways: (1) development of (joint) master programmes, (2) public availability of training materials as OER, and (3) research & development follow-on activities.

Co-funded by the European Union

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

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

Executive Summary

D6.4 captures how CyberSecPro is transitioning from project-result development to group-level exploitation, with partners jointly identifying how the project's key exploitable results can be sustained, scaled, and further developed beyond the funding period. In contrast to D6.5 (which focuses on organisation-specific exploitation), this report addresses exploitation opportunities that require shared ownership, coordinated implementation, or combined credibility across multiple consortium partners. It therefore complements the broader strategic direction of D6.3 and the partner-level roadmaps collected in D6.5.

The report follows a structured exploitation-planning logic that moves from deliverables and Key Exploitable Results (KERs) to exploitation pathways and finally to group exploitation plans. This methodology is deliberately iterative and co-created, combining ACEEU's exploitation planning experience with partner input on feasibility, sector needs, and implementation conditions. To strengthen both impact logic and implementation realism, the consortium applied a hybrid exploitation model integrating the Logic Model and the Business Model Canvas, supported by a shared exploitation canvas template for consistent planning across pathways.

As its exploitation input base, D6.4 consolidates four CSP KERs: (KER-1) the general and sector-specific cybersecurity training materials, (KER-2) the CSP certification scheme with ECSF and micro-credential/ECTS logic, (KER-3) the Dynamic Curriculum Management (DCM) system as curriculum governance and maintenance backbone, and (KER-4) the CSP state-of-the-art and best-practice reporting portfolio as an evidence and implementation resource. From this base, the report develops and clusters exploitation pathways into five thematic areas: (1) Education & Academia, (2) Open Access & Public Impact, (3) Industry & Professional Training, (4) Community Building & Engagement, and (5) Licensing & Commercialisation.

The core contribution of D6.4 is the development of detailed group exploitation plans for three priority pathways (priority given by consortium partners). First, the report outlines a pathway for a (Joint) Master Programme in Cybersecurity, with an EMJM-oriented ambition (Erasmus Mundus Joint Masters) and a parallel implementation/fallback route, grounded in CSP's curriculum and certification architecture. Second, it defines an Open Educational Resources (OER) pathway for making CSP training materials publicly available through a multi-channel model (project website, DCM, EU visibility channels, and partner/allied dissemination routes), supported by governance, licensing, metadata, and maintenance mechanisms. Third, it positions CSP as a living R&D asset portfolio, using the combined strength of all four KERs to generate follow-on projects, pilots, publications, tools, and policy-relevant outputs. Across all three plans, the report emphasises governance, ownership clarity, risk management, and lightweight monitoring as key conditions for successful post-project exploitation.

Taken together, the group exploitation plans show CyberSecPro's transition from a finite project into a coordinated exploitation portfolio: combining academic development, open public-value dissemination, and research/innovation continuation pathways. Rather than treating project outputs as standalone deliverables, D6.4 frames them as reusable and combinable assets that can be advanced through shared consortium structures, thereby strengthening the long-term sustainability, visibility, and impact of CyberSecPro in the European cybersecurity skills ecosystem

Document information

Contributors*

Name	Beneficiary
Lina Landinez	ACEEU
Thorsten Kliewe	ACEEU
Jeldo Meppen	ACEEU
Faraz Hayat	ACEEU

* The main authors and contributors would like to emphasise that all CSP consortium partners contributed to the definition of the group exploitation plans. ACEEU is mentioned above solely because it took the lead in drafting and compiling this report, and not because the underlying planning process was carried out by ACEEU alone.

Reviewers

Name	Beneficiary
Christos Douligeris	UPRC (technical lead)
Spiros Borotis	MAG (WP lead)
Alexey Kirichenko	LAU
Daniel Silveira	COFAC

History

Version	Date	Contributor(s)	Comment(s)
0.1	2025-10-06	Thorsten Kliewe	1st Draft: Add ToC; initial draft of introduction section
0.2	2025-11-18	Lina Landinez	Methodology section structured and first contents added
0.3	2025-11-19	Lina Landinez	Definition of KER added
0.4	2025-12-16	Lina Landinez	Exploitation pathways added
0.5	2026-02-12	Lina Landinez	Exploitation plans

0.6	2026-02-23	Thorsten Kliewe	Conclusion chapter added; rewriting of the introduction to reflect changes in structure and adding scoping information.
0.7	2026-02-26	Thorsten Kliewe	Added review round 1 feedback
0.8	2026-02-26	Thorsten Kliewe	Finalisation, 2nd review and high-level review approved
1.0	2026-02-28	Atiyeh Sadeghi	Final check, preparation and submission process

Table of Contents

List of Figures

List of Tables

1 Introduction

Deliverable D6.4, "Grouped Exploitation Plans", is a central component of Work Package 6 (WP6), addressing the sustainability and long-term impact of the CyberSecPro (CSP) project at group level through coordinated, multi-partner exploitation. While the project has produced a substantial portfolio of exploitable assets for European cybersecurity education and training, the post-project value of these results depends not only on individual partner uptake, but also on the consortium's ability to organise joint pathways for continuation, scaling, and wider ecosystem impact. D6.4 therefore provides a structured framework for translating CSP's Key Exploitable Results (KERs) into a set of shared exploitation pathways and, subsequently, into concrete group-owned exploitation plans. In this sense, the deliverable complements the broader strategic direction of D6.3 (consortium-level exploitation plans) and the partner-specific roadmaps documented in D6.5 (partner-level exploitation plans) by focusing on collaborative exploitation mechanisms beyond the funding period that involve some but not all CSP partners.

1.1 Background

The CyberSecPro project was initiated to address a persistent mismatch between the cybersecurity skills demanded by the European labour market and the training offers available in higher education and professional learning contexts. This challenge is particularly visible in sectors with rapidly evolving risk profiles and strong practical competence needs, such as health, energy, and maritime. CSP was designed to respond to this gap through a practice-oriented, modular, and framework-aligned approach that combines curriculum innovation, sector relevance, and public-private collaboration.

By the final phase of the project, CSP has generated a broad exploitation portfolio including:

- practical general and sector-specific training materials (KER-1),
- a certification scheme with ECSF alignment and micro-credential logic (KER-2),
- a Dynamic Curriculum Management (DCM) system as an operational backbone for curriculum governance and updates (KER-3), and
- a set of state-of-the-art and best-practice reports that provide evidence and implementation guidance (KER-4).

D6.4 is situated at the point where these results must be converted from project outputs into sustainable, jointly governed exploitation routes that can continue to create value after the project end.

1.2 Purpose and Scope

The primary purpose of this report is to document how the CSP consortium aims to translate its key results into shared exploitation pathways and concrete group exploitation plans. In contrast to deliverables that focus on individual organisational uptake, D6.4 addresses exploitation opportunities that are better pursued collaboratively, i.e. where value creation, credibility, resource requirements, or implementation feasibility depend on coordinated action by multiple partners. The report therefore moves from a project-result perspective (KERs) to a pathway perspective (strategic routes for uptake) and finally to an action-oriented planning perspective (group exploitation plans with roles, risks, and next steps). Importantly, the KERs mentioned in this deliverable differ slightly from the KERs in D6.3. Each Deliverable only refers to those KERs that are central in the respective exploitation plans.

D6.3 KER	D6.4 KER
Training Modules (KER-1)	Training Materials (KER-1)
MooCs (KER-2)	Certification Scheme (KER-2)
DCM (KER-3)	DCM (KER-3)
Certification schemes (KER-4)	CSP State of the Art and Best Practice Reports (KER-4)

This deliverable does not aim to duplicate the market-oriented analyses already provided in D6.3 (Overall Exploitation Plan). Instead, it refers to D6.3 where relevant and builds upon its findings. Similarly, the market insights presented in D2.1, D2.2, D2.3, D3.1, amongst others, are not reproduced in detail in this document, as the primary purpose of the present deliverable is to define and structure group-level exploitation planning. That said, market intelligence has informed the preparation of this deliverable throughout. In particular, the evidence generated in D2.1, together with updated market insights contributed by individual CSP consortium partners, was taken into account in the internal assessment and prioritisation process used to identify the most relevant exploitation pathways.

The scope of D6.4 includes: (a) the exploitation methodology and model used in the report (including the combined Logic Model / Business Model Canvas approach), (b) a concise presentation of the four CSP KERs as exploitation inputs, (c) a clustered set of exploitation pathways across education, open access/public impact, industry/professional training, community building, and commercialisation, and (d) a prioritised set of detailed group exploitation plans. These detailed plans focus on three consortium-level pathways: Development of (Joint) Master Programs, Making the Training Material Publicly Available, and Research & Development.

1.3 Relation with other WPs and Deliverables

D6.4 builds on outputs and experiences generated across multiple Work Packages (WP) and serves as a key bridge between CSP result generation and post-project continuation. Its main relationships are as follows:

- **WP2 & WP3 (evidence base, programme architecture, and implementation design):** D6.4 draws on the core CSP knowledge base and implementation foundations documented in deliverables such as D2.1, D2.2, D2.3, and D3.1. These outputs provide the market-demand evidence, training/programme specifications, implementation logic, and DCM-related design foundations that underpin both the KER descriptions and the rationale for the identified exploitation pathways.
- **WP4 (implementation experience and operational validation):** The feasibility and prioritisation of group pathways in D6.4 are informed by CSP's practical implementation and delivery experience during the project. These experiences provide important insight into what types of modules, formats, channels, and collaboration models are realistic for scaling and joint continuation beyond the funded period.
- **WP5 (evaluation and certification-related consolidation):** D6.4 is closely linked to D5.2 (evaluation and best practices) and D5.3 (certification schema), which are explicitly part of the CSP evidence and guidance portfolio (KER-4) and directly support the exploitation logic for several pathways. In particular, D5.3 is a key enabling input for the joint master pathway and broader certification-/ECTS-oriented exploitation options.
- **WP6 and related exploitation deliverables (D6.1, D6.3, D6.5):** D6.4 is a direct output of Task 6.3 (IPR Management and Exploitation Planning) and should be read as the group-level operationalisation of WP6 exploitation planning. It complements D6.3 (Overall Exploitation

Plan) by adding concrete multi-partner pathways and action plans, and it complements D6.5 (Individual Exploitation Plans) by focusing on shared exploitation opportunities that go beyond single-partner implementation, that is focused on the usage of the training materials. It is also aligned with the wider WP6 deliverable set, including D6.1 (Dissemination, Communication and Exploitation Plan), as part of the project's overall sustainability and impact planning.

1.4 Structure of the Report

This **Section 1 (Introduction)** sets the scene for the report. It outlines the strategic background for consortium-level exploitation planning in CyberSecPro, clarifies the purpose and scope of D6.4, and explains how this deliverable relates to the broader project work and the other WP6 exploitation deliverables.

Section 2 (Exploitation Methodology & Model) presents the methodological foundation used to develop the group exploitation plans. It describes the stepwise logic applied in this report (moving from project deliverables and KERs to exploitation pathways and then to concrete exploitation plans) and introduces the CSP exploitation model and the exploitation canvas used to support structured planning.

Section 3 (Key Exploitable Results) summarises the four CSP KERs that form the input portfolio for exploitation planning: the CSP training materials (KER-1), the CSP certification scheme (KER-2), CSP's DCM system (KER-3), and CSP's state-of-the-art / best-practice reporting portfolio (KER-4). For each KER, the report outlines its scope, strategic value, and relevance for post-project continuation, scalability, and uptake across institutions and sectors.

Section 4 (Exploitation Pathways) presents the consolidated set of pathways identified for the CSP KERs and organises them into five thematic clusters: (1) Education & Academia, (2) Open Access & Public Impact, (3) Industry & Professional Training, (4) Community Building & Engagement, and (5) Licensing & Commercialisation. The section reflects the iterative, co-creation process used with partners to refine and cluster pathways according to feasibility, relevance, and strategic fit.

Section 5 (Group Exploitation Plans) constitutes the core of the report. It develops detailed group exploitation plans for three selected high-priority pathways, covering: (1) Development of (Joint) Master Programs, (2) Making the Training Material Publicly Available, and (3) Research & Development (e.g., new research projects, publications, etc.). Each plan is presented in a harmonised structure that includes a summary (with visual overview), detailed exploitation model component descriptions, an assessment including risks, and an action plan.

Finally, **Section 6 (Conclusion)** summarises the main contributions of the report, reflects on key limitations, and outlines a future outlook for group-level exploitation of CyberSecPro results beyond the project duration.

2 Exploitation Methodology & Model

This chapter describes the methodology and model used to develop the group exploitation plans. It first explains the stepwise process applied in this report: from project deliverables and KERs, to exploitation pathways, to concrete group exploitation plans. It clarifies the key concepts used throughout. It then presents the CSP exploitation model itself, including the combined Logic Model and Business Model Canvas approach that was used to strengthen sustainability, scalability, and post-project continuation planning.

2.1 Methodology (from KER to Pathways to Exploitation Plans)

The group exploitation methodology was designed to followa simple logic: start from what the project promised to deliver (Deliverables -> KERs), translate these results into realistic and attractive routes to use (Pathways), and then convert the most attractive routes into concrete, partner-owned actions (Exploitation Plans). The approach is deliberately iterative and co-created, ensuring both consortium coherence (shared direction) and partner specificity (practical implementation by those who will exploit the results).

Core concepts and definitions as used in this report:

Key Exploitable Result (KER)

A KER is a *project result with clear potential for uptake and use beyond the project lifetime*. It is "exploitable" because it can be adopted, reused, scaled, commercialised, standardised, or institutionalised by relevant stakeholders (e.g., education providers, public bodies, industry, communities).

In this project, KERs are anchored in the funding proposal, meaning they represent the results the consortium committed to producing (e.g., training materials, certification scheme, DCM).

Exploitation Pathway (Pathway)

A Pathway is a *structured route that explains how one or more KERs can create value for specific target groups*, through a plausible mechanism of adoption and impact. Pathways describe "how exploitation could happen" at a strategic level: who benefits, what need is addressed, and what form of uptake is envisaged (e.g., curriculum integration, open access dissemination, standardisation, professional training offers).

In this project, Pathways were initially drafted based on ACEEU's exploitation experience and then refined through partner exchange and validation, including consortium discussions. This iterative process ensured the pathways reflect both market/sector realities and partner capabilities. Importantly, it also allowed the consortium to add pathways where exploitation potential became clearer over time (for example, pathways related to standardisation efforts and the (joint) master course dimension were added).

(Group) Exploitation Plan

A Group Exploitation Plan is an *action plan* (owned by more than just one CSP partner) that operationalises one or more pathways by systematically considering the relevant components and defining concrete implementation steps. It specifies what needs be done, by whom, for whom, and with what resources, including ownership considerations and feasibility checkpoints.

In this project, the exploitation plan structure (presented in Section 2.2) builds on prior ACEEU work and was shaped through exchange with project partners, resulting in a shared template that supports consistent planning while allowing flexibility across different organisational contexts.

Our stepwise approach: from KERs to pathways to plans

Step 1: Confirm and characterise the KERs (starting point: the proposal)

We began with the key deliverables/KERs defined in the proposal to ensure continuity with project commitments and expected results. This step provided a shared factual baseline: *what we have (or will have) as a result (see Chapter 3 in this report)*.

Step 2: Translate KERs into exploitation "routes" (Pathways as strategic options)

Next, we moved from results (KER) to identifying plausible exploitation routes for the KERs (see Chapter 4 in this report). This was done by combining:

- ACEEU's prior experience with exploitation and business/impact-oriented planning,
- partner knowledge of sector needs, institutional constraints, and realistic uptake conditions,
- and structured consortium discussion and refinement (including the Lisbon meeting exchange).

At this stage, pathways served two key functions:

- *Clustering and simplification*: Pathways grouped many possible uses into a manageable set of strategic options (e.g., academia uptake, open access/public value, industry training, community building, licensing/commercialisation).
- *Cross-KER logic:* Pathways make visible that exploitation often requires combining results (e.g., DCM platform plus training materials; or training materials plus certification scheme).

Step 3: Prioritise and assign ownership (from "possible" to "intended")

Not every pathway is equally relevant for every partner (and the market). We therefore used partner input to identify:

- which pathways are priority (i.e. high relevance + feasible),
- which pathways are secondary (i.e. promising but resource- or dependency-heavy),
- and which pathways require joint action (shared ownership, co-delivery, or joint credibility—e.g., standardisation).

This step bridged the gap between a consortium-wide menu of options and partner-specific intent. Ultimately, this resulted in a prioritisation as each partner was able to note their interest in each of the 20 pathways. The three highest-ranked pathways, each supported by 10 to 17 partners, were selected for further exploitation planning.

Step 4: Operationalise pathways into Exploitation Plans using a common template (Section 2.2)

Finally, each priority pathway was converted into an exploitation plan using a shared template (see section 2.2 in this report). The template supports a consistent planning logic across the consortium while asking the practical decisions that determine whether exploitation will actually happen, including:

- target group definition and access routes,
- needs addressed and value proposition,
- advancement activities required to make the KER "market-ready" or "adoption-ready,"
- additional resources and capabilities required (and whether they are available),

- roles, responsibilities, ownership and exploitation responsibility,
- risks/barriers and external landscape considerations.

This ensured that exploitation planning did not remain aspirational: each plan explicitly connected KER → pathway → actions and resources, with clear responsibility and feasibility reflection.

2.2 The CSP Exploitation Model

To develop the group exploitation plans, the CSP consortium applied a hybrid exploitation-planning methodology based on the model developed by ACEEU's EU Project Unit and further refined during the project. The methodology integrates the Logic Model (LM) and the Business Model Canvas (BMC) to ensure that exploitation planning addresses both expected impact pathways and implementation conditions for uptake and continuity.

This combined approach was used to strengthen the quality and credibility of exploitation planning by linking:

- the **intervention logic** of the project results (i.e. how results are expected to contribute to outcomes and impact), and
- the **value creation and delivery logic** (i.e. how results can be adopted, sustained, scaled, and maintained beyond the project lifetime).

The methodological integration supports a structured transition from project outputs to sustainable use, potential scale-up, and post-project continuation mechanisms, including ownership, partnerships, resources, and delivery pathways.

Logic Model

The LM is an established planning and evaluation framework used to describe how an intervention is expected to produce change over time (Public Health Ontario, 2025). It typically structures the causal chain across *inputs* (resources), *activities* (implementation actions), *outputs* (direct deliverables), *outcomes* (short- to medium-term effects), and *impacts* (long-term changes) (W.K. Kellogg Foundation, 2004).

Its principal value lies in making the project's causal assumptions explicit. By requiring a clear articulation of the relationships between resources, actions, and intended results, the LM supports internal coherence, transparency, and monitorability. It also provides a practical basis for defining milestones and assessing progress against expected outcomes.

In multi-partner settings (like the CSP project), LM is particularly useful for establishing a shared understanding of the needs addressed, the intended changes, and the respective roles of relevant stakeholders (W.K. Kellogg Foundation, 2004; OECD, 2024). It therefore supported alignment across the CSP consortium and helped ensure that exploitation planning remains anchored in agreed impact objectives rather than only in output production.

In Task 6.3 and this deliverable, the LM was used to structure each exploitation pathway by defining the required inputs and activities, the outputs to be mobilised, and the expected outcomes and impacts to be generated through implementation and use.

Business Model Canvas

The BMC is a structured framework for describing how value is created, delivered, and captured (Osterwalder & Pigneur, 2010). It consists of nine interrelated building blocks: *key partners, key activities, key resources, value propositions, customer segments, customer relationships, channels, cost structure,* and *revenue streams.*

Within exploitation planning, the BMC is particularly valuable because it introduces a practical implementation lens. It requires partners to define the conditions under which a result can move from a

project output to an adopted and maintained solution (Žlender & Erjavec, 2023). This includes clarifying:

- the target user/customer segments,
- the value proposition for each segment,
- the channels for delivery and engagement, and
- the resources, partnerships, and cost/revenue assumptions needed for continuation.

The BMC is also suitable for collaborative EU project environments because it is concise, iterative, and accessible to partners without a business background. It enables structured discussion of exploitation feasibility without requiring a full business plan at an early stage (Osterwalder & Pigneur, 2010; Žlender & Erjavec, 2023).

Importantly, the BMC helps shift the focus from the technical characteristics of a result to its user-facing value, operational viability, and continuation model. In doing so, it strengthens the basis for sustainability planning and helps identify early whether a result has realistic prospects for uptake, maintenance, replication, and scale.

Rationale for combining Logic Model and Business Model Canvas

The combined use of LM and BMC provides a more robust basis for exploitation planning than either framework alone.

The Logic Model ensures a clear articulation of the pathway from project activities to outputs, outcomes, and long-term impact. The Business Model Canvas complements this by clarifying the mechanisms through which value will be delivered, adopted, resourced, and sustained. Together, they support exploitation planning that is both impact-oriented and implementation-ready.

This combination is particularly relevant in EU projects, where exploitation planning must demonstrate not only the relevance of results, but also their feasibility for post-project continuation and their potential for wider uptake and scaling. A result may be well-positioned in terms of intended impact (LM), but still lack a credible pathway for adoption if user segments, delivery channels, ownership arrangements, or resources remain undefined (BMC). Conversely, a technically viable and commercially coherent solution may not sufficiently address broader public value, policy relevance, or long-term societal impact if only a BMC lens is applied (Verrue, 2014).

The hybrid methodology, therefore, helps address three core exploitation requirements:

- **Sustainability:** It strengthens the planning of continuation conditions by linking intended outcomes to the operational requirements needed to maintain the result over time (e.g. governance, partnerships, resources, support functions, and financing assumptions). This is aligned with the OECD DAC distinction between achieving results and ensuring their durability (OECD, 2019).
- **Scalability and transferability:** It supports early identification of factors affecting replication, adaptation, and scale-up (e.g. target segments, channels, resource intensity, partner roles, and implementation dependencies). This enables the consortium to assess whether a result can remain localised, be expanded to additional contexts, or be transferred to other organisations or territories.
- **Post-project continuation:** It provides a structured basis for defining what happens after project funding ends, including who is responsible for further deployment, how value delivery will continue, what resources are needed, and which stakeholders must remain engaged. This improves the credibility of exploitation plans and reduces the risk of outputs remaining unused after project closure.

This integrated approach is consistent with European guidance, which emphasises that exploitation planning should articulate both the societal relevance of results and a credible pathway to uptake and

use (European IPR Helpdesk, 2015; European Commission, 2021). It is also supported by applied research showing that hybrid approaches can help identify and correct imbalances between impact ambitions and operational feasibility (Lumbantoruan & Pangeran, 2021; Žlender & Erjavec, 2023).

In practical terms, the LM-BMC combination can improve the quality of exploitation planning by making critical assumptions explicit and testable. For example, an exploitation pathway may target increased uptake of a solution, but unless the BMC specifies a concrete user segment, delivery mechanism, and responsible actors, the likelihood of adoption and continuation remains weak. Likewise, an output may be strong as a project deliverable but still require substantial clarification regarding maintenance, access, support, and resourcing before it can be sustained or scaled.

This hybrid methodology was used within the CSP project as it provides a coherent framework for moving from project results to sustained exploitation. It links the impact rationale of the project (why the result matters and what change it supports) with the implementation logic required for uptake (who uses it, how it is delivered, and under which conditions it can continue and grow). As such, it strengthened the CSP consortium's capacity to develop exploitation plans that are credible, actionable, and oriented towards long-term value beyond the project duration.

2.3 The CSP Exploitation Canvas

To support the transformation of project results into usable and sustainable offers, the CSP consortium designed an Exploitation Canvas template (see figure 1), based on an earlier version from CSP partner ACEEU. The template combines elements of a logic model (input–activity–output–outcome–impact) with selected elements of business model thinking (value proposition, target-group needs, access channels, operational responsibility and feasibility considerations), as described in the previous section. This integrated structure enabled a systematic, but flexible, assessment of how CSP KERs can be further developed into products, services, operational solutions or institutional offers.

The template served both as a planning instrument and a reflection tool. It helped the CSP consortium to structure exploitation pathways, clarify assumptions, identify responsibilities, and assess whether the conditions for implementation and uptake are in place. In particular, it supported in moving beyond a result-centred perspective (i.e. what has been produced) towards an impact- and user-oriented perspective (i.e. what value can be created, for whom, and under which conditions).

The model is organised across several complementary perspectives:

- a **logic model view**, tracing the pathway from inputs and activities to outputs, outcomes and impact;
- a **product–market fit view**, focusing on user needs, value proposition and expected impact;
- a **stakeholder view**, clarifying ownership, exploitation roles, operational responsibilities and access to target groups;
- a **further insights layer**, used to capture risks, barriers and enabling factors (e.g. competition, market readiness, willingness to pay, legal or policy constraints).

Each exploitation plan begins with a short narrative description of the intended pathway, including the envisaged revenue logic and/or sustainability model where relevant. The template then guides users through the definition of expected impact, target-group needs, value proposition, required outputs, development inputs and activities, and the actors responsible for advancing, owning and exploiting the result. In addition, it prompts a structured check of feasibility, including access to required resources and access to the target group.

This approach supported a coherent and realistic exploitation strategy for the CSP project by combining strategic intent (impact and value creation) with implementation feasibility (resources, ownership, channels and operational capacity). It also facilitated consortium-level discussion and alignment, while remaining usable at partner or KER level.

Explanation of the Exploitation Canvas

The numbered circles in the template indicate a recommended working sequence, but not a mandatory order. The tool is intentionally adaptable and can be used iteratively, in parallel, or in a different sequence depending on the maturity of the KER, available evidence, and the objective of the exercise (e.g. ideation, validation, implementation planning). The recommended sequence follows an impact-led and feasibility-aware logic: first define the intended pathway and expected effects (Boxes 1–5), then identify the result base and development work needed (Boxes 6–8), and finally verify delivery conditions, exploitation capacity and governance arrangements (Boxes 9–13).

Table 1: Exploitation Template Components

Box number	Box title	Description
1	**Brief description of the exploitation path**	This box frames the pathway and explains what is to be exploited, for what purpose, and in which context. It should also summarise the intended revenue logic and/or sustainability approach (e.g. service-based, embedded institutional use, licensing, public funding continuation, mixed model).
2	**Expected impact on target group**	This box defines the intended change or benefit for the priority target group(s). It captures the expected effects of successful exploitation, including practical, organisational, educational, societal or policy-level improvements.
3	**Target group needs**	Here, the consortium identifies the needs, problems or demand conditions that the exploitation pathway aims to address. This helps ensure that the pathway is grounded in user relevance rather than solely in the characteristics of the project result.
4	**(Unique) value proposition**	This box describes the distinctive value offered to the target group, based on the identified needs. It should clarify why the proposed output is useful, credible and preferable to existing alternatives or current practice.
5	**Resulting product / service**	This box defines the concrete output to be offered (e.g. product, service, toolkit, training format, institutional process, operational solution). It translates the value proposition into a deliverable form that can be implemented, transferred or used.
6	**KER (input)**	This box identifies the relevant Key Exploitable Result(s) that form the basis of the pathway. It specifies which project result(s) will be advanced and how they relate to the intended output.
7	**Additional resources**	This box lists the extra resources required to make the KER exploitable and operational (e.g. staff time, technical expertise, legal support, funding, infrastructure, partnerships, market intelligence, certification).

8	**KER advancement activities**	This box defines the development actions needed to move from the current KER to the intended output (Box 5), such as adaptation, validation, packaging, piloting, standardisation, translation, integration or business development activities.
9	**Access to the target group**	This box assesses whether the partners have practical access to the target group(s), including channels, relationships and routes to adoption. This is a key feasibility test, as a strong value proposition alone does not guarantee uptake.
10	**Who exploits?**	This box identifies the actor(s) responsible for exploitation and operational delivery. It clarifies who will run, distribute, maintain or implement the result in practice, recognising that this may differ from the actor who developed the result.
11	**Access to required resources and capabilities**	This box checks whether the partner(s) actually own or can access the resources and capabilities listed in Box 7. It functions as a critical feasibility checkpoint and may trigger revision of the pathway where major gaps remain unresolved.
12	**Who advances the results (if needed)**	This box assigns responsibility for carrying out the advancement activities defined in Box 8. It clarifies implementation roles across partners and supports realistic planning of workload and competence allocation.
13	**Who owns the new results?**	This box clarifies ownership of the improved output/new result, including intellectual property and exploitation rights where relevant. Clear ownership arrangements are essential for sustainability, transferability and long-term exploitation.

In addition to the numbered sequence, the template includes a “further insights area” to document contextual factors that can influence exploitation success. This includes, for example, notes on competition, market maturity, willingness to pay, regulatory conditions, funding gaps, reputational factors, and other risks, barriers or drivers. Recording these factors supports more robust decision-making and helps teams refine the exploitation pathway over time.

By using this updated template, the CSP consortium assessed each priority pathway not only in terms of its internal quality, but also in relation to user relevance, implementation feasibility, sustainability, and potential impact. This strengthens the quality of exploitation planning and supports a more credible pathway from project results to long-term use and value creation.

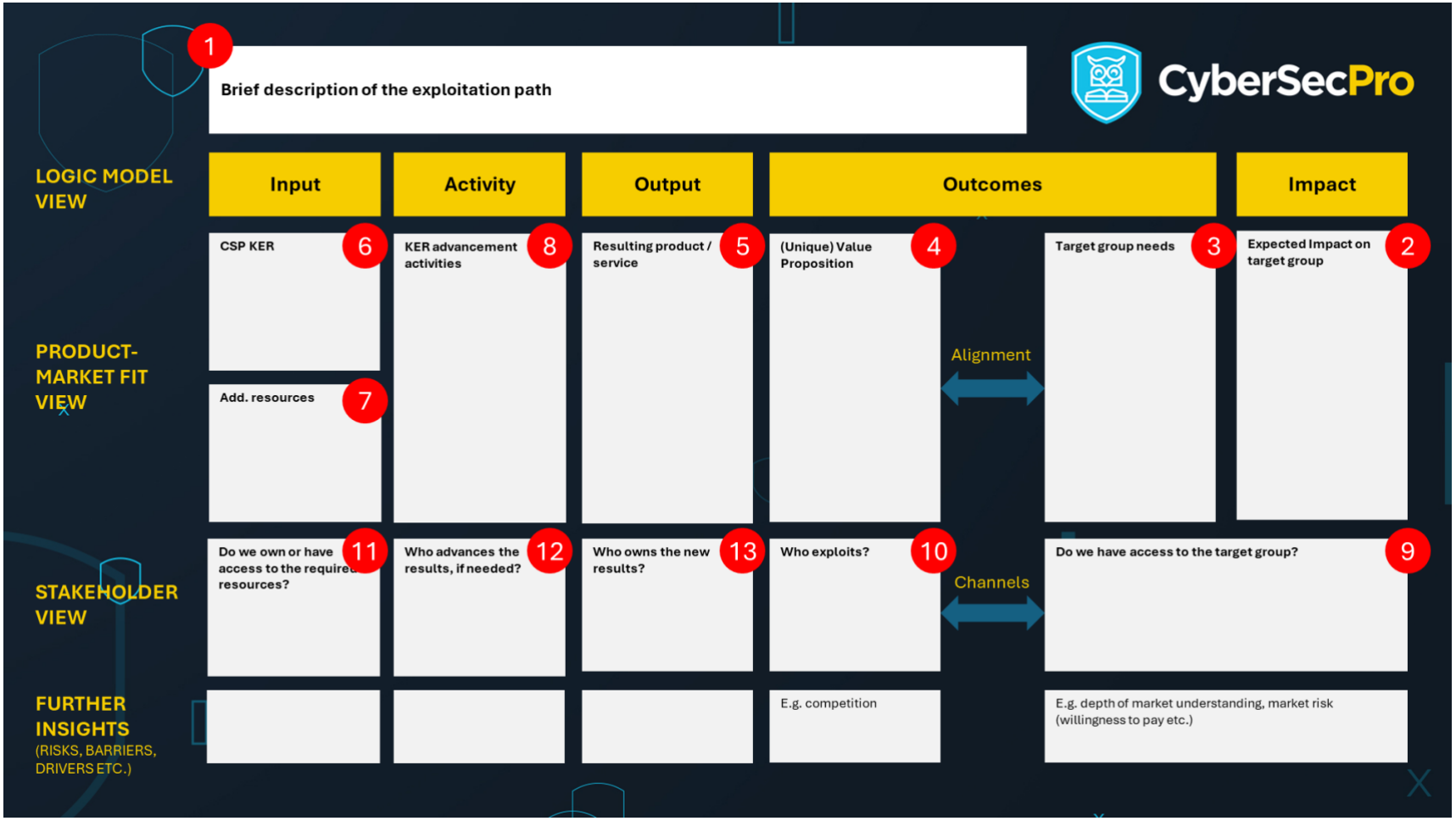

Figure 1: Exploitation Template

3 Key Exploitable Results

This chapter presents the CSP project's four KERs and summarises their strategic value for post-project uptake and continuation. For each KER, the chapter briefly describes its scope, main components, and intended users, and highlights its contribution to sustainability, scalability, and wider adoption across institutions and sectors. Taken together, the four KERs form a complementary exploitation portfolio covering training content, certification, curriculum management infrastructure, and evidence-based implementation guidance.

3.1 CSP general and sector-specific training materials (KER-1)

KER-1 comprises 72 practical training modules co-created by the CSP consortium to bridge the structural gap between academic theory and practical market needs. The content covers ten prioritised knowledge areas (e.g. Penetration Testing, Risk Management, and Incident Response) and can be offered at both basic and advanced levels to cater to diverse learner profiles. Beyond generic cybersecurity foundations, the materials are tailored for the health, energy, and maritime sectors, utilising real-life industrial scenarios and integrating specialised SME-provided tools. The materials can be (and have been) delivered through heterogeneous formats such as hackathons, seminars, and summer schools. The modules are mapped against the European Cybersecurity Skills Framework (ECSF) to ensure trainees acquire recognised, job-ready competencies for the European Digital Single Market.

3.2 CSP certification scheme (KER-2)

KER-2 is the CSP cybersecurity professional training certification scheme, developed by the CSP consortium to address fragmentation and weak interoperability of professional cybersecurity certifications in Europe, particularly in sector-specific training contexts. It provides a European-oriented certification architecture that improves consistency and mutual recognition across providers and sectors. The scheme combines modular training, micro-credentials, micro-credentials-to-ECTS mapping, and explicit alignment with ECSF roles and competences. It covers the 72 sector-specific training modules, with 14 course-type modules forming a structured pathway equivalent to 60 ECTS credits and suitable as a basis for an executive-level programme. The scheme also standardises assessment and certificate design (e.g. level, mode, workload, credits, and traceability elements), thereby strengthening comparability, transparency, and labour-market relevance, while supporting scalable, sustainable post-project exploitation across institutions and sectors.

3.3 CSP DCM (Dynamic Curriculum Management) (KER-3)

KER-3 is the CSP DCM system, developed as the operational backbone for managing and continuously updating the project's curriculum portfolio. Rather than serving as a static repository, the DCM was designed as an agile management environment that keeps training content responsive to evolving cybersecurity market needs through structured, traceable processes for curriculum versioning, governance, and quality assurance. The DCM is built on the open-source learning platform Moodle and hosted by UNINOVA. As a KER, the DCM is central to post-project exploitation because it enables sustained curriculum maintenance, quality control, and portfolio growth across institutions and public-private partnerships, thereby supporting long-term sustainability and scalable delivery of the CSP training offer.

3.4 CSP State of the Art and Best Practice Reports (KER 4)

KER4 comprises the CSP evidence base and implementation blueprints developed by the CSP consortium to align cybersecurity education and professional training with documented labour-market needs. It functions as a strategic intelligence resource for policymakers, higher education institutions, and training providers by combining market analysis, programme design specifications, evaluation findings, and certification-related guidance into a coherent reference set. Amogst others, the core outputs

include D2.1 (analysis of cybersecurity practical skills gaps and market demand in Europe), D2.2 (review of blended technological training tools and academic practice), D2.3 (programme specifications), D3.1 (programme components and procedures), D5.2 (evaluation and best practices), and D5.3 (certification schema). Taken together, these public deliverables/reports identify workforce and skills gaps, assess existing training supply and practice, define the structural and operational requirements for programme implementation, validate the CSP approach through evaluation, and provide a structured pathway for professional recognition. As a KER, this reporting portfolio supports sustainable and scalable exploitation by converting project knowledge into reusable evidence, design guidance, and implementation models for post-project continuation, replication, and wider uptake.

4 Exploitation Pathways

This chapter presents the final set of exploitation pathways identified for the CSP KERs and organises them into thematic clusters. The pathway list was developed through an iterative, co-creation process: ACEEU first prepared an initial baseline set of pathways, which was subsequently reviewed, refined, and expanded through partner input based on sector knowledge, institutional priorities, and exploitation feasibility. In a later step, the individual pathways were grouped into clusters to improve structure and usability. As several pathways can logically relate to more than one cluster, overlaps are possible; for readability, each pathway is assigned only to the cluster to which it is most strongly aligned. After presenting each pathway, the core KERs required for its implementation are mentioned.

4.1 Cluster 1: Education & Academia

1. **Integration into University and VET Curricula and Education/Training Offers**: The CSP training materials can be integrated into the partner universities' curricula and educational offers and partnering with further universities and VET institutions allows the materials to be embedded in undergraduate, postgraduate and lifelong learning /professional development programs (including Micro-credentials courses). This supports blended learning, including hybrid and flipped classroom approaches. The content can also be tailored to meet university accreditation and national education policies. KER-1 KER-4
2. **Localisation and Customisation**: CSP training materials can be adapted to regional needs, including compliance with local laws and industry-specific security concerns. Translating the content into multiple languages extends the reach to a wider global audience. KER-1
3. **Developing Cybersecurity Competency Frameworks**: The CSP materials can be used to develop standardised competency frameworks aligned with global cybersecurity standards like the NICE Cybersecurity Workforce Framework. These can serve as tools for Human Resource departments to evaluate and develop cybersecurity talent. KER-2
4. **Collaboration with Schools**: CSP materials can be adapted and used to introduce basic cybersecurity education into secondary school curricula to raise awareness at an early stage. Partnering with STEM initiatives helps promote cybersecurity as a viable and exciting career path. KER-1
5. **Development of (Joint) Master Programs**: The CSP training materials can serve as foundational content for the creation of new (joint) master's programs in cybersecurity between partner universities. These programs will incorporate CyberSecPro's modular and practice-oriented approach, ensuring alignment with emerging digital skills frameworks and industry demands. KER-1 KER-2
6. **Development of MOOCs**: Packaging the CSP materials into Massive Open Online Courses (MOOCs) allows global distribution through platforms like Coursera and FutureLearn. KER-1

4.2 Cluster 2: Open Access & Public Impact

7. **Making the Training Material Publicly Available**: Sharing CSP cybersecurity resources as OER maximises accessibility. Hosting materials on a dedicated repository enables the update of the materials and potentially also community contributions and enhancements. KER-1
8. **Making the DCM Publicly Available**: Publicly releasing the CSP DCM system enhances the project's scalability and long-term impact as organisations can easily set up an entire e-learning environment (including CSP design and settings) as opposed to integrating the CSP training materials in their own learning management system. The download options might include the DCM with all content, or the DCM without content plus separate downloads for each course (for import into the new installed DCM). KER-3 KER-1

9. **Collaboration with Non-Profit Associations**: Providing the CSP materials at little or no cost to non-profits focused on digital literacy and cybersecurity advocacy supports social impact initiatives. Training programs can help underserved communities build cybersecurity awareness and skills. KER-1
10. **Collaboration with Public Institutions**: Working with government agencies allows the CSP materials to be integrated into national cybersecurity awareness campaigns. The content can also serve as the foundation for upskilling public sector employees or supporting national defence programs. KER-1 KER-4
11. **Research and Development**: The CSP materials can serve as a foundation for further national and international research and development (projects) on cybersecurity. Collaborations with academic institutions can lead to publications, new training tools, and policy recommendations based on emerging cybersecurity trends. KER-1 KER-4
12. **Contribution to Standardisation Efforts**: The CSP materials and frameworks can inform the development of national and international cybersecurity education standards. Engagement with standardisation bodies such as ISO, CEN/CENELEC, and ETSI can ensure alignment with evolving industry and regulatory requirements. KER-1 KER 4

4.3 Cluster 3: Industry & Professional Training

13. **Industry Collaboration**: Collaborations with businesses allow customisation of the CSP training materials to meet corporate cybersecurity needs. Industry sponsorships provide funding for further content development. Corporate training packages can combine online materials with live expert sessions and practical simulations to enhance workforce skills. KER-1
14. **Cross-Sector Adoption**: Modular cybersecurity training content can be customised for different industries, going beyond the currently available materials for health, maritime and energy. Developing sector-specific case studies and role-based training ensures relevance and practical application. KER-1
15. **Offering Certification**: An (online) assessment system could provide recognised certifications upon CSP training/course completion. These certificates can be integrated into career development frameworks, aiding professionals in demonstrating cybersecurity expertise for job opportunities and career advancement. European Digital Credentials for Learning (EDC) and Europass could be used as EU-wide platforms for implementation. KER-2

4.4 Cluster 4: Community Building & Engagement

16. **Building a Learning Community**: An online learning community developed around the CSP project could encourage knowledge exchange and collaboration. Forums, webinars, networking events, and peer-driven content enhancements foster a vibrant ecosystem of cybersecurity learners and professionals. KER-1 KER-4
17. **Gamification and Simulations**: Turning the materials into interactive cybersecurity games or simulations enhances engagement. Capture the Flag (CTF) exercises, hands-on incident response simulations, and gamified learning modules could provide practical, experiential learning. KER-1
18. **Establishing a Cybersecurity Competence Centre:** Creating a national, regional or institutional cybersecurity competence centre using the training materials supports ongoing skills development. These centres can offer training programs, certifications, and consulting services for businesses and government entities. KER-1 KER-2 KER-4

4.5 Cluster 5: Licensing & Commercialisation

19. **Developing a Commercial Training Offer**: A professional CSP cybersecurity certification program can be developed targeting corporate learners. Training options include in-person and virtual workshops, boot camps, and live instructor-led sessions. Collaboration with professional organisations ensures credibility and continuing education credits. KER-1 KER-2

20. **Subscription-Based Learning Platforms**: A tiered subscription-based e-learning platform can host CSP cybersecurity training materials, offering basic access for students and advanced content for professionals. This ensures a sustainable revenue model and continuous content updates. KER-1 KER-2 KER-3

5 Group Exploitation Plans

This section presents the group exploitation plans for CyberSecPro, focusing on collaborative pathways that require coordinated action across multiple consortium partners rather than partner-specific exploitation alone. The group pathways are presented as complementary options within a broader exploitation portfolio: (1) development of a joint master programme**,** (2) open/public availability of training materials**,** and (3) research and development follow-on pathways**.** Each pathway is described using a common structure (summary, detailed exploitation model, assessment including risks, and action plan) to support comparability and implementation planning. For clarity, the plans are presented in a structured sequence, although in practice their development and execution are interdependent and iterative.

5.1 Development of (Joint) Master Programs

5.1.1 Summary (incl. Visual Overview)

The proposed exploitation pathway is to transform CSP teaching materials and the CSP certification-oriented curriculum architecture (KER-1) into a market-ready, internationally visible Joint Master in Cybersecurity, with a primary target of Erasmus Mundus Joint Master (EMJM) submission and a parallel fallback/stepping-stone route via a bilateral joint master in countries where accreditation is faster (e.g., Portugal-led route). The plan is built on the fact that CSP already has a structured curriculum basis in D5.3, including a 60 ECTS package (modules + MOOCs) mapped to the ENISA ECSF role profiles, which can be extended with 30 ECTS internship and 30 ECTS thesis/thesis preparation into a 120 ECTS master.

The plan aligns with documented market demand in Europe for hands-on cybersecurity skills (especially incident response, threat intelligence, cloud/network security, and OT/ICS-related capabilities) and sector-specific needs in health, energy and maritime/transport contexts, all of which are directly relevant to CSP's use-case orientation. CSP research (especially D2.1) and implementation experiences also support the pedagogical direction: modular pathways, practical labs/simulations/cyber ranges, challenge-based learning, and closer academia-industry collaboration.

The exploitation plan uses a mixed sustainability model rather than a single revenue source. In the launch phase, the key financial engine is EMJM funding (including programme implementation support and scholarships), while medium-term sustainability relies on a blend of tuition (self-funded and scholarship students), institutional embedding in partner HEIs, industry-sponsored internships/capstones, derivative executive/CPD offers built from CSP modules, and follow-on EU/national funding for innovation and curriculum enhancement. This is consistent with EMJM expectations that consortia plan for a sustainability/business model and institutional embedding, and with CSP's "as open as possible" dissemination logic while protecting exploitable assets and quality-controlled programme packaging.

The proposed operating model suggests a dual leadership structure: COFAC/Lusófona as academic leader (programme governance, QA/accreditation orchestration, academic integration, international consortium management) and PDMFC as practice leader (hands-on learning architecture, industry projects). Universities (LAU, UMA, UNSPMF, COFAC, UPRC) provide degree-awarding and teaching capacity, while companies and horizontal partners (PDMFC, MAG, APIRO, C2B) provide sector use cases, internships, applied labs, market alignment, QA support, and exploitation dissemination channels.

The main constraints of this pathway are not demand-side; they are execution-side: EMJM readiness requires a fully developed integrated curriculum, joint administrative/financial arrangements, mobility design, student agreements, a draft partnership agreement, and QA/accreditation evidence early in the application process. EMJM also requires compulsory physical mobility across countries and a consortium with at least 3 HEIs in 3 countries.

Overall, this exploitation pathway has a medium-high likelihood of creating real value if managed as a phased plan with explicit go/no-go gates. The strongest strategy is EMJM-first in ambition, phased in

implementation: (1) consolidate CSP into a 120 ECTS integrated design; (2) validate demand and secure industry placements; (3) complete accreditation/QA readiness; and (4) prepare an EMJM submission while retaining a bilateral joint-master fallback to ensure exploitation progress even if EMJM timing slips.

List of partners with a particularly high interest in and contributions to this exploitation pathway:

LAU, UMA, UNSPMF, COFAC, UPRC, ACEEU, APIRO, C2B, MAG, PDMFC, FCT

Group Exploitation Plans

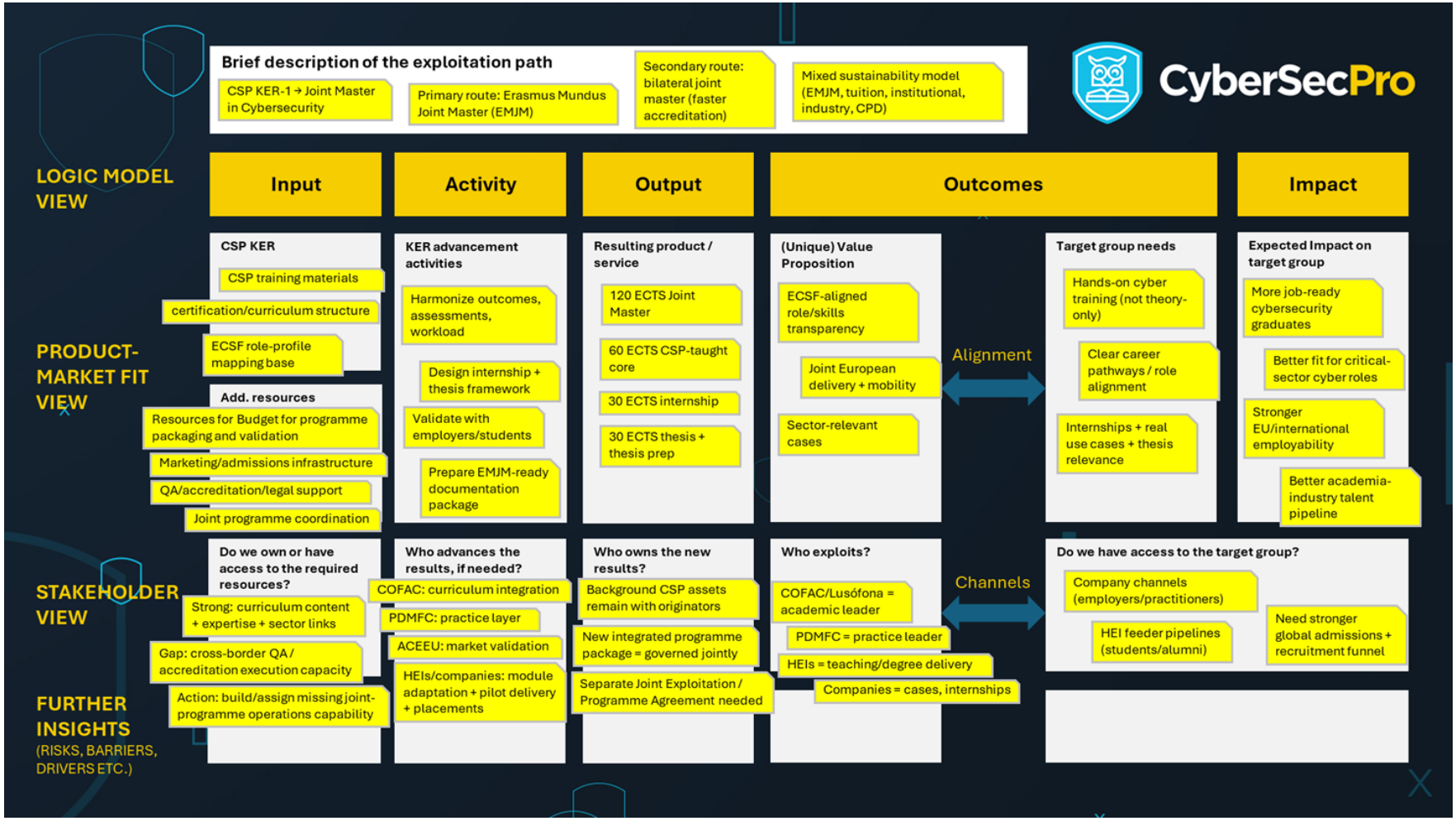

Figure 2: Joint Master Exploitation Canvas

5.1.2 Detailed Exploitation Model Component Descriptions

Note that, for ease of understanding, we have presented the exploitation plan in a sequential format (following the steps indicated in the exploitation canvas). In practice, however, the development process was iterative, and because of the interdependencies between the components of the exploitation model, the line of argumentation may not always appear fully linear.

Brief description of the exploitation path (relating to Box 1)

This exploitation pathway aims to convert CyberSecPro's KER-1 (CSP training materials and curriculum assets) into a jointly delivered European Master in Cybersecurity. The preferred route is an EMJM, because this route offers international visibility, a strong mobility narrative, and a funding framework that can support programme launch and scholarships. A secondary route is to start with a bilateral joint master's between CSP partners in countries where accreditation and implementation are faster and then expand to a broader consortium configuration. The pathway is not simply a reuse of CSP teaching materials. It is the productisation of CSP into a degree-ready programme package that includes curriculum integration, quality assurance, mobility design, internship and thesis governance, admissions assets, and operational delivery arrangements.

The revenue and sustainability logic should be designed as a mixed model rather than a single-source model. In the launch phase, EMJM funding is the strongest financial engine for programme setup and scholarships. In the medium term, sustainability should combine tuition revenue (including self-funded students), institutional embedding and co-financing within partner HEIs, industry-supported internships and capstones, derivative executive and CPD offers built from CSP modules, and follow-on EU or national funding for innovation and curriculum enhancement. This mixed approach is better suited to a cybersecurity higher-education programme than a pure licensing model, while still allowing controlled licensing of selected CSP components to affiliated institutions under a quality-managed framework.

Expected impact on target group (relating to Box 2)

For students, the expected impact is a role-oriented cybersecurity qualification that combines academic depth with demonstrable practical competence. The programme should improve graduates' readiness for cybersecurity roles aligned with ECSF, especially roles that require both technical capability and governance awareness. The intended effects are not limited to knowledge acquisition. The programme should also reduce the transition time from graduation to operational work, strengthen graduates' ability to work in multi-disciplinary teams, and increase their readiness to contribute in critical and regulated environments.

For employers, including critical infrastructure operators, public administrations, and cybersecurity service providers, the expected impact is access to a more practice-ready talent pipeline. Graduates should be better aligned with operational needs such as incident response, threat intelligence, secure architecture implementation, compliance-driven security operations, and sector-specific cyber resilience.

For HEIs, the expected impact includes a high-visibility international master's offer, stronger collaboration with industry, improved curriculum relevance, and a reusable model for future joint degree development.

For the broader European ecosystem, the pathway contributes to cyber resilience capacity building and to reducing the skills shortage in cybersecurity.

Target group needs (relating to Box 3)

The primary target group is international and European learners with a bachelor-level background who seek a career-focused master's programme in cybersecurity with strong practical components, international mobility, and clear employability outcomes. Their needs include a credible European degree, hands-on training beyond lecture-only formats, exposure to real-world scenarios, transparent career pathways, and access to internships and thesis opportunities that connect directly to labour-market needs. These needs align strongly with CSP's modular and practice-oriented design approach.

A second target group is employers and sector organisations, including public-sector and critical-sector entities, that need graduates who can work in environments shaped by NIS2 obligations, sector-specific risk management, and increasing expectations for demonstrable cyber resilience. D2.1 reinforces the relevance of this target-group definition by highlighting persistent gaps in practical cyber skills across Europe and by pointing to specific demand for capabilities such as incident response, threat intelligence, cloud and network security, and OT/ICS-related competence, especially in sectors such as healthcare, energy, and maritime/transport.

(Unique) value proposition (relating to Box 4)

The CSP Joint Master's value proposition is based on the integration of three elements that are often fragmented in existing offers. First, it provides a European multi-partner joint-delivery model with mobility and international visibility. Second, it is built on a practice-intensive curriculum architecture derived from CSP teaching materials and sector-relevant scenarios, rather than on theory-heavy modules alone. Third, it uses ECSF-aligned skills and role transparency, which makes the programme more understandable and credible to both students and employers.

Another distinctive element is the consortium composition. The CSP consortium combines universities with practice-oriented companies and a horizontal partner focused on market alignment and quality support (ACEEU). This creates a genuine bridge between degree-awarding academic institutions and real operational cybersecurity contexts. Because CSP has already produced substantial outputs (curriculum structures, modules, MOOCs, and a certification scheme), the programme can be positioned as a validated continuation of an EU-funded initiative.

Resulting product / service (relating to Box 5)

The resulting exploitable product is a Joint Master's in Cybersecurity with a target size of 120 ECTS. The intended structure is a CSP-derived 60 ECTS taught core (already structured in D5.3 and aligned to ECSF role profiles), complemented by a 30 ECTS internship or practice semester (offered by CSP companies, or non-CSP providers) and a 30 ECTS thesis and thesis preparation package. This creates a coherent full master's offer with a strong employability narrative because practical placement and advanced research work are integrated into the programme structure.

The product must be defined as more than a curriculum outline. It should be treated as a full programme package, including an integrated syllabus, module specifications, programme-level learning outcomes, ECSF mapping, admissions criteria, mobility paths, internship governance, thesis supervision rules, QA procedures, assessment policy, student agreement templates, and employer engagement mechanisms. This level of packaging is necessary to move from a project result to an exploitable, transferable, and operational master's programme.

KER (input) (relating to Box 6)

The main KER input is KER-1 and KER-2: High-quality CSP teaching materials and curriculum results (compare D5.2 for evaluation results), particularly the CSP module architecture and the certification-scheme-related structuring documented in D5.3. The D5.3 material shows that CSP already has a

coherent 60 ECTS structure consisting of modules and MOOCs, with definitions of level, delivery format, assessment logic, prerequisites, and role alignment. This substantially reduces early-stage curriculum design uncertainty and gives the exploitation pathway a strong evidence base.

A secondary input is the broader CSP project ecosystem, including industry engagement, sector use cases, and the competence base of the consortium. The CSP project has benefitted from a multi-country, multi-actor consortium spanning HEIs, companies, and sector-facing organisations. These assets can be leveraged for programme delivery, internships, mobility, dissemination, and ongoing curriculum renewal. The preliminary D6.3 exploitation work can also provide early market and pathway assumptions that can now be turned into an execution-focused exploitation plan.

Additional resources (relating to Box 7)

To make KER-1 exploitable as an EMJM-ready or joint-master-ready programme, the CSP consortium requires resources beyond the existing curriculum content. The most important additional resources are academic programme design and coordination time; QA, accreditation, and legal support across participating countries; instructional design and assessment harmonisation support; technical infrastructure for hands-on labs and cyber-range-style exercises; industry placement capacity for internships and practice projects; and marketing and admissions infrastructure for international recruitment.

Additional resources also include market intelligence and programme positioning support, which ACEEU can help coordinate, and practice-content and scenario-development capacity, which PDMFC, APIRO, C2B, and MAG can support. Since D2.1 points clearly to the need for practical and sector-contextualised cyber training, the practical layer must be resourced explicitly. Labs, simulations, challenge-based learning, and sector cases cannot be treated as ad hoc contributions if the programme is to be credible and scalable.

KER advancement activities (relating to Box 8)

The core advancement activity is to move from a CSP content portfolio to a fully integrated, jointly governed degree programme. This requires curriculum integration work, including sequencing of modules, coherence checks, removal of overlap, progression logic across semesters, and harmonisation of assessment approaches. It also requires refinement of programme-level learning outcomes and explicit mapping from modules to overall graduate profiles and ECSF role clusters.

A second critical activity is the design and standardisation of the (so far not existing) 30 ECTS internship and 30 ECTS thesis components, including supervision models, evaluation criteria, placement governance, and cross-partner consistency rules. A third activity cluster concerns validation and packaging: employer interviews, market testing, willingness-to-pay checks (either for the non-EMJM route or in preparation for the post-EMJM time), internship partner onboarding, external academic review, and pilot delivery of selected integrated modules. The final output of these activities should be a programme package that is ready for accreditation work and submission preparation.

Access to the target group (relating to Box 9)

The CSP consortium has credible initial access to the target group through multiple channels, but access is uneven and needs to be systematised. The participating HEIs (COFAC/Lusofona, LAU, UMA, UPRC, and UNSPMF) can provide access to undergraduate feeder populations, alumni networks, and academic recruitment channels. COFAC's links across institutions within the Lusofona Group are particularly valuable for scaling awareness and creating a wider student pipeline. Company partners provide access to practitioners and employer communities, which is essential for internship placement and employability signalling.

However, EMJM-level recruitment requires more than partner-local networks. It requires a globally visible programme identity, English-language positioning, a clear admissions process, and coordinated outreach to international applicants. In practical terms, the consortium already has routes to the target group, but these routes must be upgraded into a joint international admissions and outreach system with consistent messaging and clear application pathways.

Who exploits? (relating to Box 10)

The exploitation and operations model should be defined as a joint academic-practice structure with COFAC/Lusofona as academic leader and PDMFC as practice leader. COFAC could lead programme governance, consortium coordination, academic integration, QA and accreditation orchestration, and institutional embedding. PDMFC could lead the practice layer, including live cases, challenge-based formats, internship ecosystem coordination, mentor pool development, and feedback loops from employers into curriculum updates.

Operational delivery could be distributed across the consortium. The HEIs (LAU, UMA, UNSPMF, COFAC, UPRC) are the primary teaching and degree-awarding actors, subject to the final joint-programme configuration. The companies contribute structured practice input, guest teaching, case-based projects, labs, and internship placements. ACEEU could play a transversal support role focused on market alignment, quality feedback, dissemination visibility, and support for follow-on funding proposals linked to the programme's sustainability.

Access to required resources and capabilities (relating to Box 11)

The CSP consortium has strong access to core educational and domain capabilities, but only partial access to the full operational stack needed for joint-master or EMJM readiness. Clear strengths include existing CSP curriculum assets (especially the structured 60 ECTS design in D5.3), a multi-country HEI base, sector-relevant company participation, and an explicit partner role for market alignment and quality support. These strengths reduce risk in content quality, pedagogy, and labour-market relevance.

The main gaps are likely to be in cross-border accreditation and legal harmonisation, integrated admissions and registrar processes, scholarship administration, international programme marketing, and standardised internship governance across countries. The pathway is feasible, but only if the consortium explicitly assigns or acquires these capabilities in the next implementation phase.

Who advances the results (if needed) (relating to Box 12)

Responsibility for advancement should be allocated through a small execution core and thematic workstreams. COFAC, as academic lead, could chair a Programme Advancement Board and coordinate curriculum integration, governance design, and the QA/accreditation roadmap. PDMFC, as practice lead, should coordinate the Practice Integration Workstream, covering labs, scenarios, employer case input, and internship frameworks. ACEEU should coordinate a Market Alignment and Quality Feedback Workstream, including demand validation, competitor benchmarking, and evidence collection to strengthen the value proposition and market fit.

The HEIs should be assigned module or package leadership roles aligned to their strengths. LAU can support applied delivery formats and implementation pragmatics; UMA can contribute advanced cybersecurity teaching and research-linked components; UPRC can contribute applied research and community-building dimensions; COFAC can lead consortium orchestration and institutional scaling; and UNSPMF's role should be specified in the programme design stage. APIRO, C2B, and MAG should receive named responsibilities for sector-specific cases, co-teaching, capstones, and internship channels so that partner interest is converted into operational commitments.

Who owns the new results (relating to Box 13)

Ownership should be managed through a clear background IP, foreground IP, and programme-operation rights structure. Background CSP assets, including existing materials contributed by partners, should remain owned by their originating partners, subject to the project and consortium agreements. The new integrated master's package (including curriculum integration artefacts, joint administrative templates, programme branding elements, admissions processes, internship frameworks, QA protocols, and newly co-developed materials) should be governed under a dedicated Joint Exploitation and Programme Agreement.

This agreement should define rights to use, adapt, deliver, and continue the programme if the consortium composition changes. Clear ownership and usage rights are essential for long-term sustainability, transferability, and quality control. A practical approach is to keep selected learning resources open or semi-open where appropriate (in line with CSP's current Creative Commons usage), while treating the integrated programme package, quality-controlled assessments, and core operational assets as managed consortium assets with explicit licensing or access terms.

Further insights area - Risks, barriers, drivers, competition, willingness to pay (context factors)

The strongest drivers for this exploitation pathway are external and favourable: a documented cybersecurity skills shortage in Europe, policy pressure linked to NIS2 and sector resilience requirements, and growing employer demand for practical, role-ready cyber competence. The ECSF provides a strong reference framework for communicating skills alignment, while CSP's existing project outputs provide substance for fast progression from project results to an exploitable master's package.

The strongest barriers are execution-related rather than demand-related. These include accreditation and QA complexity across countries, timeline pressure for joint-programme readiness, uneven partner capacity for operational tasks, and the resource intensity of high-quality practice-based delivery. Competition from existing cybersecurity master's programmes is also relevant. CSP can mitigate this by consistently executing its differentiators: ECSF alignment, sector-specific practical training (including health, energy, maritime/transport and public-sector contexts), and a visible integration of academic and industry delivery.

5.1.3 Assessment (incl. risks)

This exploitation plan has a high likelihood of creating educational value, labour-market value, and ecosystem value, and a moderate-to-high likelihood of creating long-term financial sustainability if the CSP consortium successfully transitions from a project-result logic to an operated joint master programme model. The value creation potential is particularly strong because the exploitation pathway builds on an already developed CSP curriculum base (KER-1 / D5.3), responds to documented market demand (D2.1), and is structured around a credible European delivery model (EMJM as primary route, bilateral joint-master fallback as secondary route).

Why this is strong:

- Real market need is documented (D2.1, D6.3), especially for hands-on cybersecurity skills and sector-relevant capabilities (including health, energy, and maritime use contexts).
- The CSP content base is substantial and already structured (including a 60 ECTS foundation in D5.3), which reduces product-development risk compared to a greenfield master.
- The exploitation pathway has a clear scaling logic: EMJM-first ambition with a practical fallback route (bilateral joint master) if accreditation or timing constraints delay the EMJM route.
- Consortium diversity supports programme quality and employability, combining HEIs (degree-awarding and academic delivery) with companies (practice cases, internships, applied projects) and ACEEU (market alignment/QA support).

- The pathway aligns with EU cyber skills policy momentum (ECSF-oriented skills transparency, cybersecurity workforce development, and increasing demand under NIS2-related compliance and resilience pressures).

	Main risks / rationale	Mitigation	Overall evaluation
Technical risks	• CSP modules may remain high-quality but fragmented, without sufficient integration into a coherent 120 ECTS joint-master progression (learning outcomes, assessment logic, prerequisites, workload balance) • Internship and thesis components may be added formally but not integrated academically • Practical/lab-based delivery quality may vary across HEIs and delivery sites • Inconsistent assessment standards across partners can weaken degree credibility Rationale: The exploitation pathway succeeds only if CSP is transformed from a content portfolio into a single programme product with consistent academic and practice quality.	• Run a curriculum integration sprint (programme-level learning outcomes, semester logic, assessment harmonisation, progression map) • Define a joint internship + thesis framework with common quality criteria and supervision rules • Create a practice delivery standard (minimum lab setup, challenge format, grading principles) • Establish cross-partner moderation/review for core modules	Medium

Market risks	• Strong market need may not translate into applications if programme positioning is too generic • Competition from existing cybersecurity masters/EMJMs may reduce visibility • Student willingness-to-pay may be weaker outside scholarship-supported cohorts (a common issue in EMJM) • Employer interest may be high in principle but weak in actual internship/capstone commitments • Sector-specific differentiation may remain under-communicated Rationale: In cybersecurity education, relevance alone is not enough; positioning, trust, employability signals, and access channels determine uptake.	• Position the programme explicitly as CSP-based, ECSF-aligned, practice-intensive, and sector-relevant • Build an English-first recruitment funnel (website, admissions messaging, clear mobility and employability narrative) • Secure early employer endorsements and internship letters of intent • Package sector pathways/use cases (e.g., health, energy, maritime, public sector) • Test willingness-to-pay and sponsorship models by student segment	Medium (impact potential high, uptake quality depends on execution)
Regulatory / accreditation / operational risks	• EMJM readiness may be underestimated (integrated curriculum maturity, QA evidence, partnership agreement, mobility design, administrative setup) • National accreditation and joint-degree rules may create delays or design constraints • Administrative operations (admissions, student services, finance, mobility management) may not be sufficiently resourced • Programme launch timing may slip if approvals and governance documents are late Rationale: This is a critical feasibility risk. Many joint-programme exploitation pathways fail not because of content quality, but because accreditation and operations are treated too late.	• Treat EMJM preparation as a dedicated programme development project, not only an application-writing exercise • Build a country-by-country QA/accreditation roadmap with critical path and decision gates • Maintain a bilateral joint-master fallback route to avoid exploitation stagnation • Draft partnership agreement and operational handbook early (roles, admissions, QA, finance, student support) • Assign named leads for legal/QA/operations workstreams	Medium-high (most critical feasibility risk)

People / team / governance risks	• Key tasks may concentrate on 1–2 organisations (especially COFAC/PDMFC), creating overload and bottlenecks • Partner commitment may remain at "interest level" rather than delivery-ready effort • Responsibility for module adaptation, internships, and QA tasks may be diffuse after the project end • Delays in ownership/IP decisions may slow programme packaging and external positioning • Decision-making may become slow if all operational matters require full-consortium alignment Rationale: This is a likely failure mode in post-project exploitation: governance fatigue and unclear accountability undermine otherwise strong results.	• Create a small KER-1 Exploitation Steering Board with decision rights and monthly milestones • Convert partner interest into written commitments (role, effort, deliverables, timelines) • Assign workstream leads (academic integration, practice layer, market validation, QA/accreditation, legal/IP) • Approve a Joint Exploitation / Programme Agreement framework early • Use a readiness matrix (green/yellow/red) and escalate unresolved gaps quickly	Medium-high

5.1.4 Action Plan

The purpose of this action plan is to move from "CSP teaching materials and a 60 ECTS curriculum structure exist" to a functioning, partner-owned, and externally visible joint master's exploitation pathway (with Erasmus Mundus Joint Master (EMJM) as the primary route and a bilateral joint-master route as a practical fallback).

Table 2: Joint Master Action Plan

Phase 1 — Set up governance and confirm the EMJM-oriented pathway (Months 1–2)	
Main objective: Create the coordination and decision-making structure needed to develop the CSP joint master's and steer it toward an Erasmus Mundus application.	
Key actions • Establish a small coordination/steering group for the CSP joint master pathway (academic lead, practice lead, selected HEIs, ACEEU, and selected company partners). • Confirm the pathway scope and ambition: EMJM application as the primary target, with a practical implementation fallback route if needed. • Align the core programme concept (CSP KER-1 focus, target groups, value proposition, practical orientation). • Agree on a basic governance model (decision-making, review rhythm, partner contribution expectations). • Run an initial partner readiness scan (academic capacity, practice contribution, QA/accreditation capability, recruitment reach).	**Key results** • Agreed governance setup for the CSP joint master pathway • Confirmed EMJM-oriented exploitation route (with fallback logic) • Shared programme positioning and terminology • Initial role allocation for core and contributing partners • High-level readiness overview across interested partners
Phase 2 — Consolidate the joint master concept and build the first integrated programme package (Months 2–4)	
Main objective: Convert the CSP curriculum base into a coherent, jointly owned master concept suitable for validation and EMJM-oriented development.	
Key actions • Consolidate the CSP 60 ECTS base into a high-level joint-master architecture (including internship and thesis components toward 120 ECTS). • Define the main programme structure (taught component, practice/internship component, thesis component, mobility logic at concept level). • Align the programme concept with CSP's practical orientation and cybersecurity role/skills positioning (including ECSF-oriented framing).	**Key results** • Draft integrated CSP joint-master concept (high-level) • Agreed structure for taught / internship / thesis components • Initial ECSF-oriented positioning for employability and relevance • Shared programme concept package for validation and coordination

• Define common programme principles (learning outcomes logic, assessment coherence, partner contribution model). • Prepare an internal/external concept package for discussion with partners and stakeholders.	• List of priority issues requiring further development before application

Phase 3 — Validate market fit and prepare EMJM feasibility conditions (Months 3–6)

Main objective: Validate the attractiveness and feasibility of the CSP joint master's while clarifying the conditions needed for an Erasmus Mundus application.

Key actions	Key results
• Conduct targeted validation with employers, sector stakeholders, and academic contacts (relevance, employability, practical orientation). • Test programme positioning with prospective student audiences via partner channels. • Refine the value proposition and programme messaging based on feedback. • Clarify the main feasibility conditions for EMJM and programme delivery (high-level QA/accreditation route, consortium roles, operations model, ownership principles). • Begin building the internship/capstone opportunity pool and identifying implementation support needs	• Initial validation evidence (market relevance, attractiveness, differentiation) • Refined programme positioning and access channels • High-level feasibility path for EMJM preparation and programme delivery • Draft operational role model (academic, practice, coordination support) • Initial internship / capstone opportunity base and partner commitment picture

Phase 4 — Finalise Erasmus Mundus application package and activate implementation of the master (Months 6–12)

Main objective: Translate the validated CSP joint master concept into an EMJM application-ready package and activate the implementation pathway for the master.

Key actions	Key results
• Finalise the core programme package needed for EMJM application (integrated programme concept, consortium roles, quality/operations approach, sustainability logic at application level). • Consolidate partner commitments and contribution responsibilities for programme delivery and practice integration. • Finalise the exploitation and ownership arrangements for the integrated master package (use of CSP assets and joint programme outputs). • Prepare and submit the Erasmus Mundus Joint Master application. • In parallel, activate the implementation pathway for the master (e.g., implementation	• EMJM application package finalised and submitted (where applicable) • Confirmed implementation responsibilities across core partners • Agreed exploitation/ownership framework for the joint master package • Implementation pathway activated (including operational preparation and next-step delivery planning) • Clear transition from exploitation planning to programme implementation

	planning, partner-internal preparations, and/or fallback joint-master route steps where relevant).	

Roles and responsibilities

Core operational roles

- **COFAC / Lusófona University (academic lead):** overall academic coordination, programme integration, consortium alignment, and EMJM-oriented pathway governance.
- **PDMFC (practice lead):** practice-oriented design coordination, industry relevance, and internship/capstone pathway development.
- **ACEEU (market alignment / QA support):** support for validation, external positioning, quality-oriented feedback, and exploitation/funding follow-up**.**

Contributing roles (all interested partners)

- **Universities (LAU, UMA, UNSPMF, COFAC, UPRC):** academic input, curriculum integration support, teaching contributions, recruitment channels, and institutional feasibility input.
- **Companies (APIRO, C2B, MAG, PDMFC and others):** practice insights, sector use cases, employability feedback, dissemination through business networks, and internship/capstone opportunities.

Monitoring and review

The CSP consortium should use a lightweight monitoring approach to track progress from concept development to EMJM application and implementation activation.

Examples of indicators include:

- Governance setup and role allocation completed
- Draft integrated programme concept prepared and refined
- Validation discussions completed (employers / academic stakeholders / student-facing channels)
- Number of partners confirming contribution areas and commitment level
- Progress on feasibility conditions (QA/accreditation, operations, ownership)
- Initial internship/capstone opportunities identified
- EMJM application package readiness (milestone-based)
- EMJM application submission and implementation pathway activation status

A regular review point (e.g., quarterly) is recommended to support prioritisation, keep the pathway realistic, and ensure that exploitation planning transitions into application and implementation rather than remaining conceptual.

5.2 Making the Training Material Publicly Available

5.2.1 Summary (incl. Visual Overview)

This exploitation pathway aims to maximise the impact of CyberSecPro by making its practical cybersecurity training materials openly accessible as OER through a multi-channel distribution model:

(1) the CyberSecPro project website (ACEEU-hosted, 5+ years),
(2) the DCM platform (UNINOVA-hosted),
(3) discovery/listing via the EU Digital Skills and Jobs Platform and Cybersecurity Skills Academy ecosystem[1] (via MAG's liaison role), and
(4) third-party hosting/linking through partner and allied organisations (e.g., European Future Skills Institute).

This is a free-access pathway designed primarily for impact, reach, uptake, and reuse, with sustainability supported through partner commitments, institutional embedding, follow-on funding, and indirect commercial/public-value pathways (e.g., tailored training, certification, enterprise adaptation, platform reuse).

The pathway is strongly justified by CSP research (e.g. D2.1) and experiences made in the implementation of the modules, which document a significant cybersecurity skills gap in Europe, identify practical skills demand across sectors (including health, energy, maritime), and recommend ECSF-aligned, practice-oriented, industry-academia-connected training approaches. Best Practices identified in D5.2 (such as experiental, scenario-based learning) can also be promoted through the OER pathway.

The exploitation plan, therefore, positions CyberSecPro materials as a credible open resource base for students, recent graduates, IT/OT professionals, educators, and career changers.

To increase adoption and trust, the plan proposes a publication-ready OER packaging process: content curation, rights/IP screening, licensing decisions, metadata standardisation, ECSF role mapping, sector tags (health/energy/maritime), versioning, accessibility checks, and update ownership per module. ECSF is especially relevant because it provides a common EU reference for role profiles and skills mapping that learning providers can use to design and describe training.

The main success conditions are not technical hosting alone, but governance and operational discipline: clear responsibilities for hosting, publication QA, metadata quality, updates, platform submissions, analytics, and long-term maintenance. ACEEU, UNINOVA, and MAG form the backbone of operations/channels, while universities/research organisations and companies act as distributed content maintainers and promoters in academic and business networks. The plan also recommends a light OER Steering Group to manage release cadence and quality.

Overall, the pathway has a high likelihood of creating public value and ecosystem value, because it aligns with EU-level cyber skills priorities and visibility channels (Digital Skills and Jobs Platform / Cyber Skills Academy), and directly addresses documented labour-market needs. Key risks are uneven content updates, unclear licensing/ownership boundaries, fragmented user journeys across repositories, and weak performance tracking. These risks, however, seem manageable with the governance and 6–12 month action plan proposed below (section 5.2.5).

List of partners with a particularly high interest in and contributions to this exploitation pathway:

[1] https://digital-skills-jobs.europa.eu/en/opportunities/training/cybersecurity-fundamentals-mooc-cybersecpro , https://digital-skills-jobs.europa.eu/en/opportunities/training/zero-hero-complete-cybersecurity-toolkit-mooc-cybersecpro

TalTech, TUC, UCY, SINTEF, UNINOVA, UPRC, ACEEU, C2B, MAG, trustilio

Group Exploitation Plans

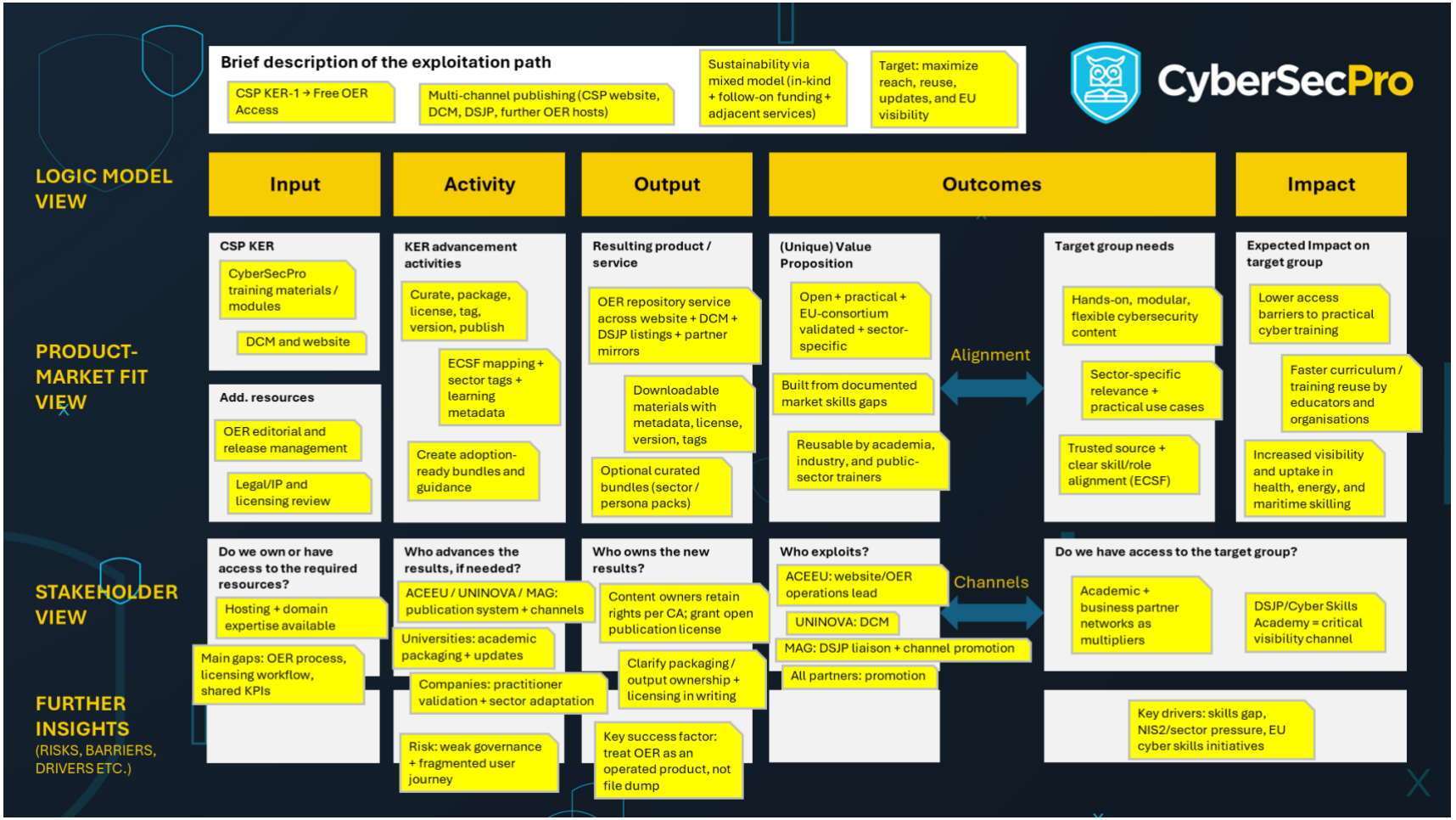

Figure 3: OER Exploitation Canvas

5.2.2 Detailed Exploitation Model Component Descriptions

Note that, for ease of understanding, we have presented the exploitation plan in a sequential format (following the steps indicated in the exploitation canvas). In practice, however, the development process was iterative, and because of the interdependencies between the components of the exploitation model, the line of argumentation may not always appear fully linear.

Brief description of the exploitation path (relating to Box 1)

This exploitation pathway focuses on making CyberSecPro training materials publicly available as OER to maximise reach, uptake, reuse, and long-term impact across European cybersecurity education and training ecosystems. The pathway exploits the project's practical training outputs by packaging and publishing them in a way that is easy to discover, download, reuse, and periodically update. The intended context is European cybersecurity workforce development, especially for skilling, upskilling, and reskilling in sectors such as health, energy, and maritime, where CyberSecPro already generated sector-relevant content and market evidence.

The sustainability logic is a mixed public-value model rather than a direct paywall model. Core materials remain free to access as OER, while sustainability is supported through:

- partner-hosted infrastructure commitments (ACEEU website, UNINOVA DCM),
- institutional embedding in curricula and training offers,
- public/EU follow-on projects, and
- indirect value capture through adjacent exploitation pathways such as customised training delivery, enterprise services, certification, and platform deployment.

This is consistent with the D6.3 emphasis on diversified/scalable business models and public-private balance, but adapted here to a free OER-first pathway.

The pathway is also aligned with OER good practice: openly licensed educational materials need clear governance, licensing, and dissemination mechanisms to remain usable and trusted over time. UNESCO's OER Recommendation provides the policy-level rationale for openly licensed educational resources, while Creative Commons licensing provides the practical legal mechanism for reuse.

Expected impact on target group (relating to Box 2)

The expected impact is improved access to practical, market-relevant cybersecurity training materials for a broad set of European learners and intermediaries (educators, institutions, trainers, companies). For learners, the main change is lower access barriers to high-quality, practice-oriented cybersecurity content; for educators and training providers, the change is faster curriculum enhancement and easier adoption of sector-specific practical modules; for organisations, the change is improved availability of reusable training assets for internal capacity building. D6.3's target-group framing (students, recent graduates, IT/OT professionals, and career changers) supports this broad impact logic.

At ecosystem level, the pathway can help reduce fragmentation in training supply by making CSP materials more visible through EU-level channels such as the Digital Skills and Jobs Platform and the Cyber Skills Academy environment. These channels for training opportunities, learning content, and community/networking, which makes it a strong dissemination and uptake channel for this pathway.

A realistic impact expectation is not "solving the cyber skills gap alone" but contributing a credible, reusable, sector-aware practical resource base that strengthens education/training offers and supports workforce development initiatives in multiple Member States. D2.1 already documents the scale and persistence of the problem and recommends collaborative, practical, ECSF-informed responses; this pathway directly serves that recommendation set.

Target group needs (relating to Box 3)

The target groups for this pathway include (1) students and recent graduates, (2) IT/OT professionals and mid-career practitioners, (3) educators/trainers and universities, (4) companies and public-sector organisations needing training content, and (5) intermediaries/platforms that curate learning content. Across these groups, the common needs are: practical hands-on content, flexible modular access, sector relevance, credible sources, and training aligned to job roles and market demand. D2.1 and experiences made throughout the CSP project strongly support these needs and specifically highlights demand for practical skills and the gap between market needs and current academic supply.

Sector-specific needs are especially important. D2.1 shows differentiated emphasis in health, energy, and maritime (e.g., management/tools and ethical hacking in health and energy; maritime emphasis on management systems, tools/processes, awareness, engineering). This means the OER publication approach should not present the materials as a single undifferentiated library, but as a tagged, role- and sector-oriented resource set.

There is also a policy/compliance demand driver that increases the relevance of practical cybersecurity training: the EU's NIS2 framework spans 18 critical sectors, and sector-specific regulatory/industry requirements (including maritime cyber resilience developments such as IACS E26/E27) create ongoing training needs in operational contexts. This does not automatically create demand for free OER, but it increases the likelihood that organisations will search for practical training content and baseline materials.

(Unique) value proposition (relating to Box 4)

The unique value proposition of this pathway is: open, practical, EU-developed, sector-specific cybersecurity training materials that can be directly reused, adapted, and integrated by educators, institutions, and organisations, with credibility from a multi-partner European consortium and strong alignment to real workforce needs.

This value proposition is differentiated in several ways. First, the materials are grounded in a project (CSP) that explicitly analysed European cybersecurity skills demand/supply gaps and focused on practical skills in health, energy, and maritime. Second, the consortium combines universities/research organisations and companies, which supports relevance and credibility across both academia and practice. Third, the open publication pathway lowers adoption barriers and enables downstream reuse. D2.1 and D6.3 together support these differentiators.

A further strengthening element is ECSF-informed tagging/mapping. ENISA's ECSF is the EU reference point for cybersecurity professional roles and skills and is explicitly positioned as a tool for training providers to design and describe programmes. Mapping materials to ECSF roles makes the OER more legible to employers, educators, and learners.

Resulting product / service (relating to Box 5)

The resulting product is not a single course, but a multi-channel OER publication and access "service" for CSP training materials. In practical terms, this includes:

- a curated OER section on the CyberSecPro website,
- downloadable materials via the UNINOVA-hosted DCM (login-based but free),
- discoverability listings on the Digital Skills and Jobs Platform / Cyber Skills Academy ecosystem,
- mirrored or linked hosting by partner/allied organisations (e.g., European Future Skills Institute), and
- an operating process for updates, metadata, quality assurance, and analytics.

The "service" component means: users need not only files, but also a usable access pathway (searchability, tags, versioning, descriptions, licensing clarity, and stable links). The Digital Skills and Jobs Platform's structure (training opportunities + learning content catalogues) makes it a relevant visibility channel, but because it acts "only" as a discovery layer, CyberSecPro's own channels must remain the authoritative storage and update points.

To improve long-term discoverability and citation, the plan also recommends (optional but high value) an archival mirror for selected stable releases in a trusted repository (e.g., Zenodo/OpenAIRE ecosystem) with versioned records and citations, while keeping the website/DCM as operational distribution channels.

KER (input) (relating to Box 6)

The core input KER for this pathway is the CyberSecPro training material set (the publicly shareable modules and associated resources; KER-1), which has been proven to be of high quality (e.g. knowledge-transfer scores between 6.0-6.92 on a 7-point scale, see D5.2). A secondary enabling input is the DCM platform capability (UNINOVA), which supports hosting and structured access.

Additional resources (relating to Box 7)

To make the KER fully exploitable as a high-quality OER offering, additional resources are required beyond "just uploading files." The most important are: editorial/product management time, technical publishing support, metadata and taxonomy work, legal/IPR review, licensing decisions, accessibility QA, translation/localisation prioritisation (where needed), analytics/dashboard setup, and communications/promotion capacity.

A legal and governance resource is especially important because public OER publication requires clear rights and licensing status for each module/component (text, slides, images, datasets, lab instructions, third-party tools/screenshots, logos, etc.). Technical and metadata resources are also critical. For this pathway, minimal and privacy-safe analytics instrumentation (e.g., country/institution collection on download forms, aggregate reporting) should be implemented with clear privacy notices and purpose limitation.

KER advancement activities (relating to Box 8)

The advancement activities should convert "project training outputs" into a robust, reusable OER product set. This should include a structured pipeline: content triage (potentially including content improvement based on WP5 evaluation results and recommendations) and content selection, public-release packaging, rights/IP screening, license assignment, metadata tagging, sector and ECSF mapping, accessibility review, versioning, publication to website/DCM, and DSJP listing preparation. This is the key step that translates project outputs into a reusable exploitation-ready asset.

A practical recommendation is to define a publication standard for every item: title, short description, target audience, sector tags, ECSF role tags (where applicable), skill level, format, prerequisites, estimated learning time, language, license, version/date, owner/maintainer, and citation/reference information. ENISA ECSF and the DSJP's catalogue logic make this especially valuable for discoverability and comparability.

A second advancement stream should focus on adoption readiness, not only content packaging. This includes creating "starter bundles" (e.g., health/energy/maritime starter packs; educator pack; SME pack), short guidance on how to integrate materials into courses or internal training, and partner-ready communication assets.

Access to the target group (relating to Box 9)

This pathway is strong on access because the consortium already has multiple complementary channels to reach the target groups. The four defined channels create a good portfolio of direct distribution (website/DCM), EU-level discoverability (DSJP/Cyber Skills Academy), and external amplification (partner/allied hosts). This reduces dependence on any single platform and increases resilience.

In particular, access is strengthened by the fact that the Digital Skills and Jobs Platform is a major EU digital skills hub and includes learning content and training catalogues, while also serving the broader Digital Skills and Jobs Community and the Cyber Skills Academy environment. This is highly relevant for educators, institutions, and professionals searching for trusted content.

The CSP consortium's partner mix is also a strong access asset. Universities and research organisations can drive uptake in academic networks and curriculum integration; companies can drive uptake in business networks, professional training, and sector-specific contexts. CSP partner-specific interests (e.g., SINTEF maritime/competence center opportunities, MAG's municipal/customer reach, ITML/APIRO/C2B/FP/TRUSTILIO's training and industry links) materially improve access feasibility if coordinated through a common campaign and update process.

Who exploits? (relating to Box 10)

The operational exploitation model should be distributed with a clear backbone:

Backbone operations (central):

- ACEEU: Website OER section hosting and operational stewardship (front-end access, publication pages, download funnel, analytics summary, public-facing OER governance coordination), with the stated maintenance commitment for at least 5 years.
- UNINOVA: DCM operational hosting and technical administration (account access, repository structure, platform uptime, backup, technical publishing support for DCM-distributed materials).
- MAG: Liaison/entry point for Digital Skills & Jobs Platform submissions and promotion alignment (including Cyber Skills Academy-related visibility opportunities), plus dissemination in MAG's customer/business ecosystem.

Note: Allowing community contributions would introduce a key operational challenge: submissions must be reviewed by the host to ensure relevance, quality, and alignment with the initiative's objectives.

Distributed exploitation operations (content/network level):

- Universities and research organisations (TalTech, TUC, UCY, UPRC, UNINOVA, SINTEF): Academic promotion, curriculum-facing reuse, upload/update of materials they own or co-own, educator outreach, and quality feedback.
- Companies (APIRO, C2B, FP, ITML, MAG, TRUSTILIO): Business-network promotion, professional-training adaptation signals, update contributions, and sector-specific use-case amplification.

Access to required resources and capabilities (relating to Box 11)

The CSP consortium has access to most required capabilities, but not all at the same maturity. Core strengths: technical hosting capability (ACEEU website; UNINOVA DCM), sector/domain knowledge across academia and industry, dissemination channels, and real use-case proximity in multiple sectors.

The likely capability gaps are more operational than strategic: consistent OER metadata management, rights-clearing discipline, editorial release management, multilingual prioritisation, and shared

analytics/KPI reporting. These gaps require explicit assignment and a lightweight process to address the pathway risks becoming a static “file dump” instead of a maintained exploitation asset.

Who advances the results (if needed) (relating to Box 12)

Advancement activities should be allocated by capability, not just by original authorship. A practical allocation is:

- ACEEU (lead, with MAG and UNINOVA): Advance publication readiness model (OER templates, publishing workflow, metadata standard, website structure, governance process, KPI dashboard specification).
- UNINOVA (lead for DCM technical advancement): DCM taxonomy/category structure for OER, user flow optimisation, access/logging setup, integration support for public-facing references, backup/versioning procedures.
- MAG (lead for external channel advancement): DSJP listing preparation workflow, quality of entries, metadata harmonization for external catalogue submission, dissemination packages for business audiences, and channel promotion.
- Academic/research partners (TalTech, TUC, UCY, UPRC, UNINOVA, SINTEF): Academic adaptation and quality refinement, curriculum-use packaging, sector/evidence annotations, educator guidance notes, update commitments for selected materials.
- Company partners (APIRO, C2B, FP, ITML, MAG, TRUSTILIO): Practitioner-facing packaging refinements, sector-specific application notes, industry validation feedback, and identification of "high uptake" modules for prioritised improvement.

Who owns the new results (relating to Box 13)

Ownership and exploitation rights must be clarified at two levels: content ownership and publication-layer/packaging ownership.

For the training materials, the suggested approach is that original content-owning partners (or jointly owning partners) retain ownership according to the consortium agreement and background/foreground rules, while granting a non-exclusive open license for public OER publication and reuse (in line with the already chosen Creative Commons Licence). This follows the CSP proposal's idea of being "as open as possible".

For newly created packaging outputs (metadata schema, OER guidance, publication templates, website descriptions, downloadable bundles), ownership can either remain with the creating partner(s) or be assigned/jointly managed as CSP consortium exploitation assets (with clear licensing). The key goal is that ownership must not block publishing and updating.

For infrastructure:

- Website hosting operations remain with ACEEU (service/hosting responsibility, not ownership of all content).
- DCM platform technical ownership/custodianship remains with UNINOVA for the platform layer, with content rights remaining with content owners.
- External listings (DSJP) do not transfer content ownership; they are discoverability entries pointing users to the authoritative CSP channels.

Further insights area - Risks, barriers, drivers, competition, willingness to pay (context factors)

This pathway benefits from strong structural demand drivers. D2.1 documents the skills gap and practical training needs, while EU-level cyber skills initiatives (Cyber Skills Academy) and digital skills channels (DSJP) improve visibility and policy alignment. Regulatory and sector developments (e.g., NIS2 across 18 sectors, maritime cyber resilience requirements under IACS UR E26/E27, and broader CRA-related compliance pressures for digital products) also sustain demand for cybersecurity upskilling content and practical awareness materials.

The biggest barriers are not demand, but execution quality and governance. If licensing is unclear, materials are hard to find, or updates stop, the perceived value declines quickly. Another barrier is fragmentation: users may encounter multiple entry points (website, DCM, external links) and lose trust if navigation, versions, or metadata are inconsistent.

Competition is real but mostly complementary in this OER pathway. The main alternatives are commercial training providers, large MOOC platforms, and institutional/internal training libraries. CSP does not need to outcompete them on brand or polish across all domains; it can win on sector relevance, practicality, openness, and EU consortium credibility, in line with D6.3's competitive differentiation logic.

Willingness to pay is less relevant for the core OER path (free access), but highly relevant for adjacent services. The intended approach is: use the OER pathway to drive impact and trust, and let paid/customised exploitation happen in adjacent pathways, not by compromising openness, but to support long-term sustainability through revenue generation.

5.2.3 Assessment (incl. risks)

This exploitation plan has a high likelihood of creating value in terms of public value, educational value, and ecosystem value, and a moderate likelihood of creating direct standalone financial sustainability if assessed as a pure OER channel only.

Why this is strong:

- Real market need is documented (D2.1), and validated through module implementations during the project implementation.
- The content base is substantial and sector-specific.
- Multi-channel access is already designed, including an EU-level discoverability route.
- Consortium diversity supports distribution and reuse across academia and industry.
- The pathway aligns with EU cyber skills policy momentum (ECSF/Cyber Skills Academy context).

	Main risks / rationale	Mitigation	Overall evaluation
Technical risks	• Fragmented user experience across website / DCM / external listings • Broken links, outdated files, inconsistent versions • Weak metadata/searchability (users can't find relevant modules) • Access friction in DCM login flow reduces uptake • Inadequate analytics makes decisions guess-based Rationale: The OER path succeeds on discoverability and trust. If users cannot find or confidently reuse materials, the value proposition will not become reality.	• One canonical URL per item + versioning policy • Metadata standard and tagging taxonomy (sector, level, ECSF role, format) • Automated link checks and repository QA • Low-friction download flow on website • Common KPI dashboard across website/DCM/DSJP referrals	Medium
Market risks	• High competition/noise in online cybersecurity training • OER users may browse but not adopt/reuse deeply • Materials may feel too broad unless packaged by persona/sector • Rapidly changing threats/regulations may age content Rationale: In cybersecurity, freshness and applicability are essential. "Free" is not enough; relevance and usability drive adoption.	• Prioritise high-demand sectors/use cases identified in D2.1 • Publish curated starter bundles (health/energy/maritime, educator, SME) • Use ECSF tagging to improve clarity and alignment • Promote "living repository" positioning rather than static archive	Low-medium for impact, medium for uptake quality)
People / team / governance risks	• Unclear ownership/licensing approvals delay publication • Update responsibilities become diffuse after the project end • Core operational work falls onto 1–2 partners • Partner motivation varies if OER benefits are indirect • No decision forum for prioritisation and conflict resolution Rationale: This is the most likely failure mode. OER exploitation may fail due to governance fatigue, not lack of content or market need.	• Create a small OER Steering Group (ACEEU, UNINOVA, MAG + 2 content partners) • Assign module maintainers and backups • Approve a publication checklist and rights workflow • Track partner contributions and reuse cases to maintain momentum	Medium-high, and the most critical

Summary:

If the consortium treats this as an operated product (with governance and release discipline) rather than a one-time dissemination task, it is very likely to create meaningful value and strengthen the overall CyberSecPro exploitation portfolio.

5.2.4 Action Plan

The purpose of this action plan is to move from "materials exist" to a functioning, visible, and maintainable OER exploitation pathway.

Table 3: OER Action Plan

Phase 1: Set up governance and common rules (Months 1–2)	
Main objective: Create the basic coordination and decision-making structure needed to operate the OER pathway.	
Key actions • Establish a small coordination group for the OER pathway (e.g., ACEEU, UNINOVA, MAG + selected content partners). • Confirm the final scope of the pathway and align terminology. • Agree on a common publication approach for openly sharing materials. • Define a shared structure for how materials will be described (metadata/tags) and maintained.	**Key results** • Agreed governance setup • Shared publication principles (including licensing and rights checks) • Common metadata/tagging structure • Agreed roles for core operational partners and contributing partners
Phase 2: Prepare materials and channels for publication (Months 2–4)	
Main objective: Convert the project outputs into publication-ready OER assets and prepare the delivery channels.	
Key actions • Select and prioritise materials for the first release (what is ready now, what needs improvement, what comes later). • Prepare the first set of materials for public release (packaging, descriptions, version/date, ownership/maintainer information). • Set up / refine the OER section on the CyberSecPro website (ACEEU). • Set up / refine the DCM access and structure for OER materials (UNINOVA). • Ensure consistency between channels (website, DCM, external listings).	**Key results** • First release set of OER-ready materials • Website OER section ready for use • DCM structure for OER access ready for use • Initial internal quality checks completed

Phase 3: Activate dissemination and external visibility (Months 3–6)	
Main objective: Make the materials visible and usable through the consortium and external channels.	
Key actions • Prepare and publish key listings via the Digital Skills & Jobs Platform channel (via MAG). • Launch a partner dissemination push through academic and business networks. • Encourage third-party hosting/linking arrangements (where appropriate). • Publish a small number of curated entry points (e.g., sector-oriented bundles such as health, energy, maritime).	**Key results** • First wave of external listings/live references • Partner promotion activities underway • Additional hosting/linking relationships activated • Curated access points that improve usability and uptake
Phase 4: Review uptake, improve, and secure continuity (Months 6–12)	
Main objective: Consolidate the pathway by reviewing usage, improving materials, and formalising sustainability arrangements.	
Key actions • Review basic usage and reach indicators (e.g., downloads, registrations/accesses, countries/institutions represented, referrals, reuse examples). • Identify which materials should be updated, improved, or archived. • Run a second improvement/release cycle for priority materials. • Agree on a medium-term sustainability and maintenance approach (roles, commitments, review cycle, future funding opportunities). • Formalise post-project continuity arrangements for hosting and update responsibilities.	**Key results** • Initial evidence of uptake and reuse • Priority updates / second release wave • Agreed continuity and maintenance approach • Clearer pathway from OER visibility to broader exploitation opportunities

Roles and responsibilities

Core operational roles

- **ACEEU**: Website OER hosting and public-facing coordination
- **UNINOVA**: DCM hosting and technical repository support
- **MAG**: External platform liaison (Digital Skills & Jobs Platform) and dissemination support

Contributing roles (all interested partners)

- **Universities / research organisations**: content updates, academic dissemination, curriculum-related reuse

- **Companies**: practitioner feedback, sector dissemination, business-network promotion, use-case validation

Monitoring and review

It is recommended to use a lightweight monitoring approach to track whether the pathway is working.

Examples of indicators include:

- Number of materials published
- Usage/access indicators across website/DCM
- Number of countries/institutions reached
- External listings published
- Examples of reuse in courses/training contexts
- Update status of key materials

A regular review point (e.g., quarterly) is recommended to support prioritisation and continuous improvement.

5.3 Research & Development

5.3.1 Summary (incl. Visual Overview)

This proposed exploitation pathway positions the CSP consortium not only as a provider of cybersecurity training content, but as a European R&D platform for evidence-based, sector-specific cybersecurity skills innovation. The pathway is built on a combined use of all four KERs: KER-4 (evidence base and implementation reports) and KER-1 (72 practical modules) serve as the primary research substrate; KER-3 (DCM) serves as the operational infrastructure for continuous curriculum evolution, experimentation, and traceability; and KER-2 (certification scheme) provides a strong basis for research and pilots on certification interoperability, micro-credentials, recognition, assessment quality, and pathways into executive/professional programmes.

The exploitation logic is to turn CSP from a completed project into a living R&D asset portfolio that can generate:

1. new EU/national projects,
2. scientific publications,
3. demonstrators and digital tools (e.g., AI-enabled lab training support, adaptive learning pathways, sector simulation/gamification extensions, curriculum intelligence tools),
4. policy and implementation recommendations for cybersecurity upskilling, and
5. transferable models for universities, training providers, clusters, and industry.

The target groups are not limited to learners. They include HEIs, RTOs, cybersecurity SMEs, sector operators (health/energy/maritime), public authorities, and policy actors that need practical, standards-aware, updatable cybersecurity training and credentialing approaches. The CSP consortium has strong access channels through universities, industry clients, sector clusters and networks, professional training channels, and existing cross-sector relationships.

A key strength of this pathway is its combined value proposition: few consortia can offer, at once,

- an evidence base on skills gaps and implementation (KER-4),
- validated hands-on sector-specific modules (KER-1),
- an operational curriculum management backbone (KER-3), and
- a structured European-oriented certification architecture with ECSF alignment and micro-credential logic (KER-2).

This allows the CSP consortium to move faster from problem identification to pilot design to funded R&D proposal submission and deployment.

The pathway is suitable for a portfolio of upcoming opportunities. Most relevant are Horizon Europe Cluster 3 (ECCC-linked cybersecurity R&I topics) in the 2026 work programme (including software/hardware security, SecureAI, and advanced cryptography topics), Digital Europe / ECCC cybersecurity deployment calls, DIGITAL-2026-SKILLS-09 (Advanced Digital Skills) for ecosystem coordination and competitions, and selected Erasmus+ 2026 actions for educational innovation, policy experimentation and wider uptake. While the focus may primarily be on education–oriented R&D calls, CSP insights could also strengthen proposals under calls that prioritise the technical development and deployment of cybersecurity solutions (e.g. by designing relevant educational materials).

The plan is seen as viable and potentially high-value, but only if the consortium moves quickly on three fronts in the next 6–12 months: (1) topic selection and positioning, (2) governance and ownership rules for follow-on R&D outputs, and (3) a proposal pipeline with named leads and bid/no-bid gates. Otherwise, the pathway risks remaining a broad intention rather than an operational exploitation route.

List of partners with a particularly high interest in and contributions to this exploitation pathway:

GUF, LAU, TalTech, TUC, UCY, UMA, UNSPMF, SINTEF, UNINOVA, UPRC, ACEEU, APIRO, C2B, FP, ITML, MAG, trustilio, SLC

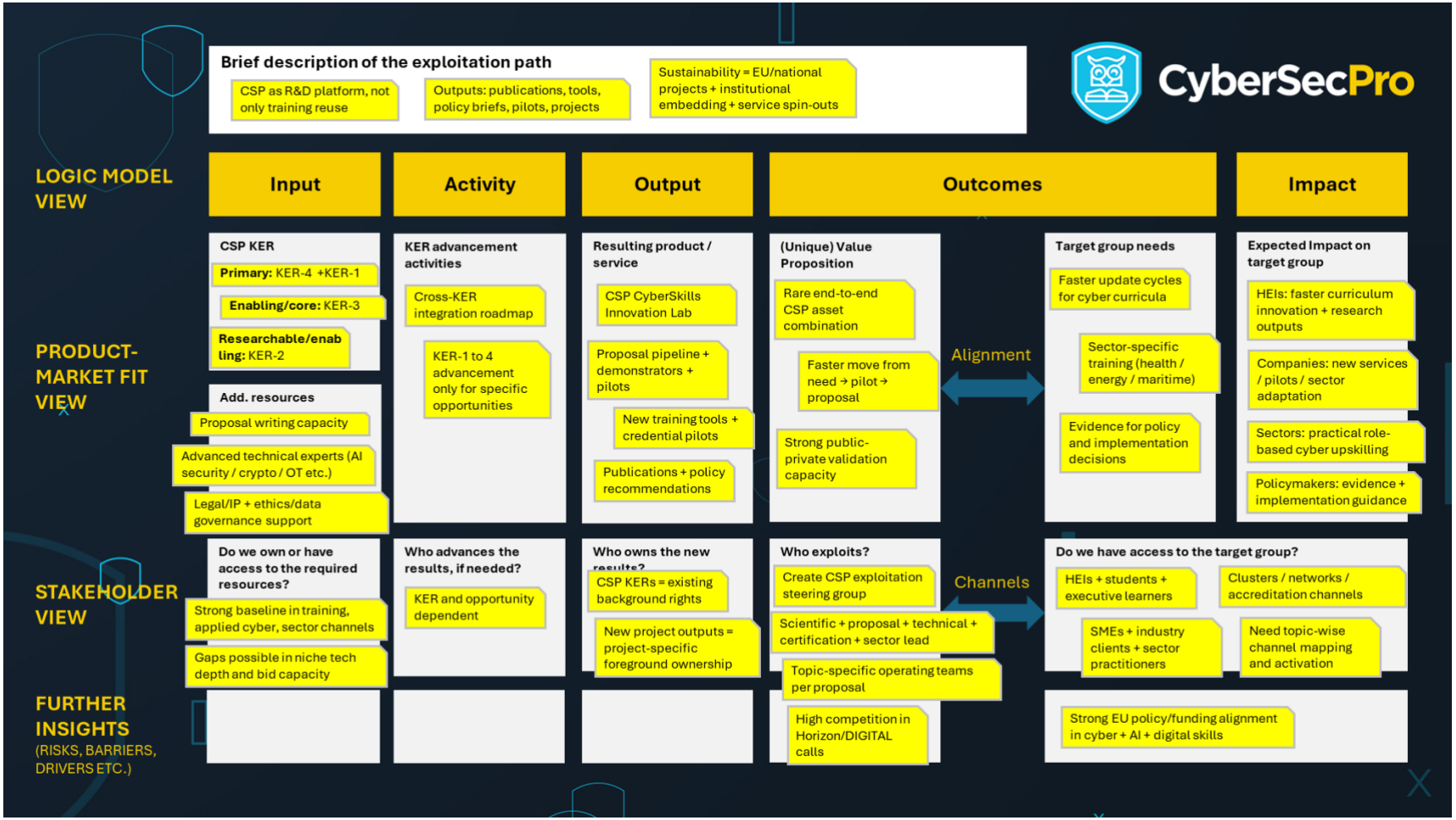

Figure 4: R&D Exploitation Canvas

5.3.2 Detailed Exploitation Model Component Descriptions

Brief description of the exploitation path (relating to Box 1)

This exploitation path focuses on using the CSP results as a structured foundation for future cybersecurity research and development projects, at European and national level, with the explicit aim of generating new scientific, technological, educational, and policy outputs. The pathway is not limited to reusing CSP teaching assets. It treats the CSP results as an integrated innovation stack: KER-4 provides the evidence base and implementation intelligence; KER-1 provides validated practical modules and sector scenarios; KER-3 (DCM) provides the operational environment to manage evolution and experimentation of curricula; and KER-2 provides the certification and credentialing architecture that can be researched, tested, and further developed in future projects.

The exploitation pathway is therefore a research-to-deployment cycle: identify new cybersecurity skills or technology needs (e.g., secure AI, post-quantum migration readiness, OT/ICS resilience, cyber range pedagogy, sector-specific incident response exercises), formulate an R&D concept grounded in CSP evidence and assets, run pilots/conduct projects, and publish/transfer the results into new training tools, policy recommendations, and further funding proposals.

The revenue/sustainability logic is a mixed model. Direct commercial revenue is not the main driver in this pathway. Sustainability comes from:

- follow-on R&D funding (EU, national, regional, sectoral),
- institutional embedding of CSP-derived assets in university and professional programmes,
- co-funded pilots with industry/public sector stakeholders,
- consulting/training spin-out opportunities for CSP companies based on newly developed results,
- and research publications, demonstrators, and policy outputs that reinforce the consortium's attractiveness for future consortia.

In other words, the exploitation path is sustainable if it creates a self-reinforcing loop between funded R&D projects, curriculum/tool evolution, and market/policy relevance.

Expected impact on target group (relating to Box 2)

The expected impact differs by target group but follows a common logic: the CSP consortium will help organisations move from fragmented or outdated cybersecurity training practice toward evidence-based, sector-relevant, continuously updateable and recognisable skills development pathways.

For higher education institutions and research organisations, the impact is the availability of a strong basis for new applied research projects, publications, thesis topics, and curriculum innovation, especially where cybersecurity skills development intersects with AI, sector regulation, simulation/gamification, micro-credentials, and labour-market alignment. For universities such as TUC, UCY, UPRC, LAU, GUF, UMA, and others, this pathway strengthens their role in both academic research and practice-oriented cybersecurity capability building.

For cybersecurity companies and training-oriented SMEs in the CSP consortium, the impact is the ability to co-develop and test new service formats, sector-specific training solutions, tooling integrations, and adoption models, which can later be commercialised or embedded into service portfolios. This is particularly relevant for partners with strong applied and sectoral connections (e.g., APIRO, ITML, FP, MAG, Trustilio, C2B).

For sector stakeholders (health, energy, maritime and potentially adjacent domains such as aviation/public administration), the impact is improved access to practical, role-based, standards-aware training and new tools that are derived from actual operational needs and tested in realistic settings.

For policymakers and ecosystem actors, the impact is the availability of updated evidence, implementation guidance, and policy recommendations on how to improve cybersecurity skills systems, credential recognition, and sector-specific workforce development.

Target group needs (relating to Box 3)

This pathway addresses a set of recurring needs in the European cybersecurity education and workforce ecosystem. A central need is the persistent mismatch between formal education delivery and rapidly evolving operational cybersecurity requirements, especially in sector-specific settings and in practical, hands-on capability development. The CSP project was designed precisely to address this gap, and the R&D pathway extends that logic by turning CSP results into a platform for further experimentation and adaptation.

HEIs and training providers need faster curriculum update cycles, stronger linkage to real operational scenarios, better methods for evaluating practical competence, and credible pathways for micro-credentials and recognition. This is where the combination of KER-1, KER-2, and KER-3 becomes especially relevant.

Industry stakeholders and sector operators need usable, role-based training approaches that can be adapted to their constraints (time, operational risk, regulatory requirements, workforce profiles, maturity levels), rather than generic awareness content. They also need evidence on what works in adoption and upskilling, not just content libraries.

Policy and ecosystem actors need evidence-backed recommendations on skills development, certification comparability, and scalable implementation models. This need is directly supported by KER-4, and strengthened when KER-4 is continuously refreshed through follow-on R&D activities.

Finally, the consortium itself needs a pathway that converts project outputs into a strategic positioning asset for future funding and collaboration. The R&D exploitation path meets that need by making CSP a launchpad for new consortia and funded initiatives.

(Unique) value proposition (relating to Box 4)

The unique value proposition of this pathway is that the CSP consortium can offer an end-to-end R&D foundation for cybersecurity skills innovation, rather than isolated assets. Many (research) groups can offer training content; fewer can offer content plus certification logic; even fewer can combine that with a living curriculum management system and a documented evidence/implementation portfolio.

The distinctiveness lies in the integration of all KERs:

- KER-1 gives the consortium a substantial, practical, sector-specific module base (not just concepts),
- KER-2 adds a structured, ECSF-aligned certification and micro-credential architecture,
- KER-3 enables continuous adaptation, governance and scaling of curriculum assets,
- KER-4 provides the analytical and implementation evidence to justify and shape new research directions.

This makes the CSP consortium highly competitive for R&D topics that require demonstrable maturity, stakeholder realism, and cross-sector transferability. It also supports a stronger proposition to funding bodies: CSP is not asking to start from scratch, but to advance and validate an already structured European asset base.

Resulting product / service (relating to Box 5)

The resulting exploitable output can be best described as a CSP R&D exploitation programme (or "CSP CyberSkills Innovation Lab" model) rather than a single product. It is a coordinated exploitation mechanism through which the CSP consortium develops and offers:

- new R&D proposals and project concepts,
- demonstrators and prototypes (e.g., training support tools, analytics components, adaptive pathways, simulation/gamification extensions),
- validated sector-specific training innovations,
- publications and conference outputs,
- and policy/implementation recommendations.

KER (input) (relating to Box 6)

This pathway should explicitly use all KERs, with differentiated roles.

KER-4 (CSP State of the Art and Best Practice Reports) is a primary input because it provides the evidence base, implementation logic, and validated insights needed to identify high-value research directions and justify proposals. It should be treated as the strategic intelligence layer for future project ideation, policy recommendations, and methodological grounding.

KER-1 (CSP general and sector-specific training materials) is also a primary input because it provides the practical substance for experimentation, piloting, adaptation, evaluation, and extension. The modules enable the consortium to build follow-on R&D around concrete teaching and operational artefacts rather than abstract curricula.

KER-3 (CSP DCM) is an enabling input and, in some topics, also a direct research object. It supports versioning, governance, quality assurance, and continuous curriculum maintenance. In future projects, it can be further developed into a stronger platform for curriculum analytics, traceability, interoperability, and secure multi-partner management.

KER-2 (CSP certification scheme) is both an enabling and researchable input. It can support future work on certification comparability, micro-credentials, assessment quality, recognition pathways, ECSF alignment, and executive/professional programme structures. In some proposals, the certification scheme itself can be a central innovation target (e.g., pilots on recognition, portability, stackability, or sector-specific credential pathways).

Additional resources (relating to Box 7)

To make this pathway operational, the CSP consortium will need resources beyond the existing KERs. The first resource category is proposal and portfolio development capacity: dedicated staff time for call scanning, concept note drafting, consortium building, budgeting, and proposal writing. Without this, the pathway will remain opportunistic.

A second category is research and technical development capacity, including cybersecurity domain experts, instructional designers, software/platform developers (especially if KER-3 is extended), evaluation experts, and data/learning analytics expertise. For cybersecurity R&D topics involving AI security, cryptography, or sector testbeds, specialised technical expertise will need to be assembled per proposal.

A third category is legal/governance support, including IP and exploitation rights arrangements, data governance (especially if learner or usage data are used in pilots), ethics procedures, and agreement templates for multi-partner follow-on projects.

A fourth category is market and stakeholder engagement resources, including access to pilot sites, sector operators, SMEs, professional learners, and public authorities. These channels exist across CSP partners, but they must be operationalised.

Finally, the consortium may require platform and infrastructure upgrades, especially if the DCM is used as a collaborative R&D backbone (e.g., metadata enhancements, APIs, stronger traceability, analytics modules, multilingual handling, access control hardening, integration with assessment/credential tools).

KER advancement activities (relating to Box 8)

The advancement activities for this pathway should be treated as a staged, proposal-driven workstream, not as a mandatory full upgrade of all KERs before exploitation can begin. In many follow-on R&D opportunities, the CSP KERs can already be used effectively as background assets with limited advancement. Therefore, the consortium should distinguish clearly between (a) minimum exploitability

readiness activities that are needed now, and (b) targeted enhancement activities that are only undertaken when justified by a specific call, pilot, or funded project.

Access to the target group (relating to Box 9)

The feasibility of this pathway is strong because the CSP consortium has multiple access routes to relevant target groups, although these routes need to be organised more systematically.

On the academic side, universities in the consortium provide access to students, academic staff, executive learners, thesis supervision structures, and research collaboration channels. This is particularly important for piloting and evaluation, publication generation, and proposal consortia formation.

On the industry side, CSP companies provide access to SMEs, clients, sector practitioners, and professional learners, including consulting/training customers and operational environments where cybersecurity upskilling needs are concrete and immediate. Some partners also have strong sector-specific entry points (e.g., maritime, energy, municipalities/public administration, human-centric cybersecurity training contexts).

On the ecosystem side, the consortium has access through clusters, networks, accreditation and engagement channels, which supports scaling, stakeholder recruitment, and dissemination.

While access exists, it needs to be mapped, segmented, and activated for this pathway. A practical next step is a target-group/channel matrix for each priority R&D topic.

Who exploits? (relating to Box 10)

Operational exploitation of this pathway should be led by a small cross-partner exploitation steering group, rather than being left fully decentralised. The pathway is inherently distributed, but it needs coordination to avoid fragmentation and duplicated proposal efforts.

A good operational model is:

- one scientific/exploitation coordinator (overall pathway management and bid pipeline governance),
- one funding/proposal coordination lead (call intelligence, proposal calendar, bid support),
- one technical integration lead for KER-1/KER-3 coherence,
- one certification/credential lead for KER-2-related opportunities,
- and one sector/pilot engagement lead coordinating access channels.

In practice, exploitation delivery will then vary by proposal/topic:

- CSP universities will typically lead research design, evaluation and publications;
- CSP companies will lead deployment validation, sector adaptation and client-facing pilots;
- Network-oriented partners (e.g., ACEEU) will support visibility, dissemination and consortium formation;
- UNINOVA (and relevant technical partners) will play a central role where DCM evolution is part of the pathway.

Access to required resources and capabilities (relating to Box 11)

The CSP consortium has a strong baseline for this pathway. The consortium has access to cybersecurity teaching expertise, practical training delivery channels, sector engagement in key domains, and academic research capacity. It also has relevant strengths in applied R&D, serious games/gamification, consulting/training, and cross-sector transfer.

Potential gaps may arise especially in:

- advanced technical niches needed for specific calls (e.g., high-assurance cryptography, secure AI engineering, formal methods),
- productisation-grade software development if DCM/tooling extensions become ambitious,
- dedicated bid management capacity.

Group Exploitation Plans

Who advances the results (if needed) (relating to Box 12)

Advancement responsibilities should be assigned by KER and by topic theme.

- For KER-1 advancement, responsibility should sit with the universities and companies that own/maintain the most relevant CSP modules for a chosen theme (e.g., sector-specific content owners, technical SMEs, teaching leads).
- For KER-2 advancement, responsibility should be led by partners most closely involved in certification design, academic recognition processes, and credential implementation, with participation from HEIs that can test institutional recognition and from companies that can validate labour-market relevance. The lead should be taken by UPRC who led the development of the certification scheme.
- For KER-3 advancement, responsibility should be led by UNINOVA as the partne who provided technical stewardship of the DCM and platform operations , with support from content owners and other partners to ensure that technical changes are aligned with pedagogical and exploitation needs.
- For KER-4 advancement, responsibility should be led by research-oriented universities capable of market analysis, methodological updates, and policy-oriented synthesis, while sector and company partners contribute current field intelligence and validation. LAU might take the lead as the core partner behind the creation of D2.1.

Who owns the new results (relating to Box 13)

Ownership arrangements for the R&D pathway must distinguish clearly between:

1. existing CSP background results (the four KERs), and
2. new foreground results created in follow-on projects.

The CSP KERs remain under the ownership and rights framework already defined by the CSP consortium and related agreements. Any new proposal should explicitly state which KER components are contributed as background and under what access/use conditions.

For new results emerging from follow-on R&D (e.g., adapted modules, new software components, analytics extensions, assessment methods, policy frameworks, new certification extensions, demonstrators), ownership should be defined in each project's consortium agreement and exploitation plan from the start. In this pathway, ownership will likely be mixed:

- academic partners may own publications/methods,
- technical partners may own software/tool components,
- multiple partners may co-own integrated outputs,
- and some outputs may be intentionally made open (e.g., policy briefs, selected educational artefacts) to support impact and adoption.

Further insights area - Risks, barriers, drivers, competition, willingness to pay (context factors)

A major driver is the continued European policy and funding focus on cybersecurity, digital resilience, AI security, digital skills, and critical infrastructure protection, which supports the relevance of the CSP consortium's profile and assets. The Horizon Europe Cluster 3 2026 work programme includes ECCC-linked cybersecurity topics in software/hardware security, secure AI, and cryptography with published 2026 timetable information, which is directly relevant for this pathway's R&D positioning.

Another driver is the availability of complementary pathways under DIGITAL Europe and ECCC implementation lines, including the broader Digital Europe work programme framework and ECCC cybersecurity deployment calls, plus Advanced Digital Skills call opportunities that can strengthen ecosystem-building and skills-related scaling.

Key barriers include consortium coordination overhead, topic diffusion ("too many possible ideas"), and the risk of trying to package CSP as a generic training project instead of a differentiated cybersecurity R&D platform. Competition is high, especially in Horizon Europe and DIGITAL Europe calls; successful proposals will need a sharper technical focus and stronger evidence of operational access and deployment feasibility. A further risk is that KER-3 and KER-2 remain underused in proposals if the consortium defaults to content-only narratives.

A practical mitigation is to define 2–3 priority R&D themes and force each theme to explicitly state how all relevant KERs are used (primary, enabling, or optional), instead of assuming a one-size-fits-all exploitation story.

5.3.3 Assessment (incl. risks)

This exploitation plan has a high likelihood of creating value in terms of research value, public value, educational value, and ecosystem value, and a moderate likelihood of creating direct standalone financial sustainability if assessed as a pure "proposal-generation" pathway only. It becomes significantly stronger financially when treated as a portfolio pathway that combines follow-on R&D funding, co-funded pilots, institutional embedding, and service spin-outs (e.g., sector adaptation, validation, certification support).

Why this is strong:

- Real market and skills need is documented (especially practical cybersecurity skills gaps and sector-specific needs), and CSP already generated usable assets and implementation experience to respond to it.
- The CSP asset base is unusually strong because it combines all KERs, not only content: KER-1 (training modules), KER-2 (certification scheme), KER-3 (DCM), and KER-4 (evidence and best-practice reports).
- The consortium has multi-channel access to academia, RTOs, companies, sector stakeholders, and training audiences, which supports pilots and proposal credibility.
- The pathway supports both research and implementation outcomes (projects, demonstrators, publications, policy recommendations, and new training/certification tools).
- The pathway aligns with ongoing EU cybersecurity and digital skills momentum, including ECSF-oriented approaches, sector resilience needs, and cyber capacity-building priorities.

	Main risks / rationale	Mitigation	Overall evaluation
Technical risks	• Weak integration across the four (or at least more than one) KERs (content, certification, DCM, evidence base) leads to fragmented proposal narratives • KER-3 (DCM) may be treated as a repository only, instead of an R&D-capable curriculum management backbone • Limited evaluation instrumentation/data governance reduces ability to prove impact • Topic ambitions (e.g., SecureAI, PQC, OT/ICS) may exceed available technical depth in a given consortium configuration Rationale: This pathway depends on credible, integrated use of all relevant KERs. If the technical and methodological foundations are not clearly packaged, proposals may look generic or underpowered.	• Create a four-KER architecture template for each proposal (what is primary, enabling, optional) • Build a KER-3/DCM enhancement roadmap focused on proposal-enabling upgrades (metadata, traceability, workflow, analytics hooks) • Use minimum viable pilots to validate KER-2/KER-3 claims before scaling • Prepare a standard evaluation + ethics/data governance package for pilots • Add external specialist partners where needed (instead of stretching CSP beyond its strengths)	Medium
Market risks	• High competition in Horizon / DIGITAL calls • Topic diffusion (too many possible R&D ideas, weak prioritisation) • Proposals framed around “training supply” rather than sector operational pain points • Follow-on outputs may attract interest but not sustained adoption without clear host/owner • Rapid technology and regulatory change can make themes stale if not refreshed Rationale: R&D exploitation succeeds only if CSP is positioned as a differentiated cybersecurity innovation platform, not a generic training consortium. Funding-fit and target-group relevance are decisive.	• Limit the pathway to 2–3 priority R&D themes at a time • Use target-group validation interviews (sector operators, SMEs, HEIs, public actors) before full proposal drafting • Apply a formal bid / no-bid gate (call fit, KER leverage, pilot access, technical credibility) • Maintain a living KER-4 evidence refresh to keep themes current • Pair major EU bids with smaller national/sector pilots to generate evidence and de-risk future submissions	Medium (funding conversion), Low-medium (impact relevance if focus is maintained)

People / team / governance risks	• No clear operating structure for the pathway (everyone interested, nobody accountable) • Proposal writing and exploitation work added on top of existing workloads without protected capacity • Uneven partner engagement over time • Unclear ownership and background/foreground rules for four-KER reuse in follow-on projects • No decision forum for prioritisation, conflict resolution, or contribution tracking Rationale: This is the most likely failure mode. R&D exploitation pathways usually fail due to governance fatigue and coordination overload, not because the KERs are weak.	• Create a CSP R&D Exploitation Steering Group (small core, named roles) • Assign topic owners and proposal owners for each theme/call • Reserve protected effort for bid development and pathway coordination • Prepare a standard KER background-use + IP principles template for follow-on projects • Use a regular portfolio review (themes, calls/bids, risks, partner contributions, resource gaps) • Track visible outputs (concept notes, proposals, pilots, publications) to maintain momentum	Medium-high, and the most critical

Summary

If the CSP consortium treats this pathway as an operated R&D portfolio (with governance, prioritisation, and proposal discipline) rather than a broad intention to "do more projects," it is very likely to create meaningful value and significantly strengthen the overall CyberSecPro exploitation portfolio through the combined use of KER-1, KER-2, KER-3, and KER-4.

5.3.4 Action Plan

The purpose of this action plan is to move from **"CSP KERs exist"** to a functioning, coordinated, and credible **R&D exploitation pathway** that can generate follow-on projects, pilots, publications, and related exploitation opportunities.

Table 4: R&D Action Plan

Phase 1: Set up governance and common pathway rules (Months 1–2)	
Main objective: Create the basic coordination and decision-making structure needed to operate the CSP R&D exploitation pathway.	
Key actions • Establish a small coordination group for the R&D pathway (representing research, technical/platform, certification, and sector-facing perspectives). • Confirm the pathway scope and shared terminology (including consistent reference to all relevant CSP KERs). • Agree on a simple working model for how R&D opportunities will be identified, prioritised, and pursued. • Define a common structure for describing proposed R&D themes (problem, target group, KER use, expected outputs, likely funding route).	**Key results** • Agreed governance setup for the CSP R&D exploitation pathway • Shared pathway scope and terminology • Simple decision process for opportunity selection (e.g., bid/no-bid) • Common concept-note structure for future R&D themes
Phase 2: Map KERs and prepare the pathway for proposal development (Months 2–4)	
Main objective: Translate the four CSP KERs into a usable exploitation base for future R&D proposals and pilots.	
Key actions • Create a practical four-KER exploitation map (what is reusable now, what may require further advancement, and where each KER fits best). • Identify a small set of initial R&D theme areas (e.g., technology-driven, sector-driven, or certification/credentialing-focused themes). • Map consortium capabilities and access channels to those themes (academic, industry, public-sector, sector-specific).	**Key results** • Four-KER exploitation map (KER-1, KER-2, KER-3, KER-4) • Initial shortlist of priority R&D theme areas • Partner capability and access overview linked to themes • Draft common principles for KER reuse in follow-on proposals

• Clarify basic assumptions on background use of CSP KERs and expected ownership handling for new results in follow-on projects.	

Phase 3: Activate dissemination and external visibility (Months 3–6)

Main objective: Convert the pathway into a small but credible pipeline of external opportunities and collaboration-ready concepts.

Key actions	Key results
• Scan and shortlist relevant funding opportunities (EU/national/regional) for the selected themes. • Prepare a limited number of concept notes (high level, not full proposals yet). • Validate the themes informally with selected stakeholders (e.g., sector contacts, training users, academic peers, industry partners). • Prepare a short CSP R&D positioning message/material that explains the four-KER exploitation logic for external collaboration and proposal building.	• Shortlist of relevant funding / programme opportunities • First concept notes for priority themes • Initial external feedback on relevance and feasibility • CSP R&D pathway positioning material for partner outreach / consortium building

Phase 4: Launch first proposal/pilot activities and consolidate continuity (Months 6–12)

Main objective: Move from planning to execution by launching the first proposal and/or pilot activities, and formalising how the pathway will continue.

Key actions	Key results
• Select the first priority opportunity (or small set of opportunities) for active proposal development. • Assign clear lead and contributing roles for proposal/pilot preparation. • Use the selected theme(s) to define which CSP KERs require immediate advancement (if any) before submission/piloting. • Review progress and refine the pathway based on early experience (what worked, what did not, where gaps remain). • Agree on a medium-term continuity approach for the R&D pathway (coordination, review rhythm, and resourcing expectations).	• First proposal and/or pilot activity launched • Clear role allocation for active opportunity development • Initial lessons learned for improving the pathway • Agreed continuity approach for the CSP R&D exploitation pathway

Roles and responsibilities

Core operational roles

A small coordination group should take operational responsibility for the R&D exploitation pathway. The exact composition can remain flexible, but it should cover at least:

- Scientific/exploitation coordination (overall steering)
- Proposal/funding coordination (opportunity scanning and proposal process support)
- Technical/platform perspective (especially where KER-3 / DCM is relevant)
- Certification/credential perspective (especially where KER-2 is relevant)
- Sector/pilot engagement perspective (industry and end-user access routes)

Contributing roles (all interested partners)

- Universities / research organisations: research themes, publications, validation approaches, academic pilots, curriculum integration, evidence updates
- Companies / industry-facing partners: sector needs, practitioner feedback, pilot environments, applied use cases, deployment feasibility, market relevance
- Network / dissemination-oriented partners: external visibility, consortium building support, stakeholder engagement, pathway communication

Monitoring and review

The CSP consortium should use a lightweight monitoring approach to track whether the R&D exploitation pathway is functioning. Examples of indicators include:

- Number of R&D themes scoped and prioritised
- Number of concept notes prepared
- Number of opportunities screened / shortlisted
- Number of active proposal or pilot preparations launched
- Number of partners actively contributing to pathway work
- Evidence of external interest (e.g., stakeholder feedback, collaboration discussions)
- Progress in using/advancing relevant KERs within the pathway

A regular review point (e.g., quarterly) is recommended to support prioritisation, coordination, and continuous improvement. The aim is not heavy reporting, but ensuring that the pathway remains focused, active, and connected to real exploitation opportunities.

6 Conclusion

6.1 Contributions

This report consolidates the group-level pathways from CyberSecPro result generation to post-project value creation by translating the project's KER into structured exploitation pathways and then into concrete, group-owned exploitation plans. In doing so, D6.4 complements the overall exploitation direction of D6.3 and the organisation-specific focus of D6.5 by addressing exploitation opportunities that require coordinated action, shared governance, and combined partner credibility. Rather than treating exploitation as a generic "next step," the report operationalises it as a portfolio of pathways with explicit responsibilities, risks, and implementation logic.

A key contribution of D6.4 is methodological. The report introduces and applies a stepwise exploitation-planning logic (from deliverables/KERs to pathways to exploitation plans) supported by a hybrid model combining LM and BMC. This approach strengthens both impact-orientation and implementation realism: it helps the consortium move beyond listing possible uses of project outputs and instead specify target groups, value propositions, operational requirements, governance arrangements, and feasibility conditions for post-project continuation. The shared exploitation canvas further supports consistency across pathways while still allowing adaptation to different exploitation logics (public-value, academic, R&D, and mixed sustainability models).

A second major contribution is the consolidation of exploitation options into a manageable and strategic pathway structure. By clustering exploitation opportunities (e.g., academia, open access/public impact, industry/professional training, community-building, licensing/commercialisation), the report creates a practical bridge between a broad set of CSP assets and a realistic set of consortium priorities. This pathway approach is especially valuable because it makes cross-KER logic visible: several of the most promising exploitation options rely not on a single KER, but on combinations of content, certification, DCM, and evidence/implementation knowledge.

The core practical contribution of D6.4 is the development of detailed group exploitation plans for three priority pathways:

- **Development of (Joint) Master Programs** (EMJM-oriented with a bilateral fallback route),
- **Making the Training Material Publicly Available** (OER-first, multi-channel dissemination and maintenance model), and
- **Research & Development** (positioning CSP as a living R&D asset portfolio combining all four KERs)

Across these plans, the report makes an important shift from "output completion" to "operated exploitation." It explicitly addresses governance and steering structures, ownership and IP clarity, phased 6–12 month action plans, lightweight monitoring indicators, and risk mitigation measures. This is particularly relevant in multi-partner exploitation contexts, such as the CSP project, where failure is often caused less by weak results and more by unclear accountability, coordination fatigue, or delayed operational decisions. D6.4 therefore provides not only strategic direction, but also a practical execution frame for post-project continuation.

6.2 Limitations

The main limitation of D6.4 is that it is, by design, a planning and coordination deliverable, not an implementation results report. The group exploitation plans define credible pathways, roles, and action sequences, but they do not yet provide evidence of execution outcomes (e.g., confirmed programme launches, measured OER uptake at scale, or successful proposal awards). This is appropriate for the purpose and timing of the deliverable, but it means that the report should be read as a structured commitment and decision-support instrument rather than proof of realised post-project impact.

A second limitation is that exploitation maturity and implementation certainty differ across pathways. The joint master pathway has a strong value proposition and a clear phased plan, but its execution depends on demanding feasibility conditions such as accreditation/QA readiness, administrative operations, partner commitments, and timing alignment for an EMJM submission. Similarly, the OER pathway is comparatively strong on public-value logic and operational setup, yet still depends on licensing clarity, update discipline, and consistent multi-channel user journeys. The R&D pathway has significant portfolio potential, but its success depends on prioritisation, governance capacity, and conversion of broad themes into focused proposals/pilots with named leads and bid/no-bid decisions. In short, D6.4 documents strong pathways, but not equal levels of execution risk across them.

A third limitation concerns the level of detail that can be included in a public deliverable. Some exploitation-relevant elements (especially partner-specific resource allocations, internal decision thresholds, detailed financial assumptions, and certain IP/ownership negotiation positions) are either intentionally kept at a strategic level or deferred to follow-up agreements and implementation workstreams. This is visible, for example, in areas where ownership frameworks are defined as principles that require later formalisation in dedicated agreements for programme operation or follow-on R&D projects. As a result, the report improves clarity significantly, but it does not (and should not) replace the legal, operational, and financial documents needed for execution.

6.3 Future outlook

The next 6–12 months will be the critical period for converting the group exploitation plans from strategic intent into operational post-project activity. The report shows that CyberSecPro has generated a strong and versatile asset base; however, long-term impact will depend on the consortium's ability to move from planning to execution through clear governance, timely decisions, and focused implementation. In particular, the transition from project closure to post-project exploitation requires lightweight but effective coordination structures, named responsibilities, and realistic prioritisation of actions.

A key success factor for this next phase will be maintaining momentum while avoiding coordination overload. Multi-partner exploitation often fails not because of weak results, but because responsibilities remain too broad, decision-making is delayed, or operational follow-up is fragmented. The group exploitation plans in D6.4 provide a solid foundation to address these risks, but their value will ultimately depend on disciplined follow-through, regular review, and the willingness of partners to align around a manageable number of shared priorities.

Looking ahead, CyberSecPro seems well positioned to evolve from a time-bound project into a reusable and adaptable exploitation portfolio with continued relevance for the European cybersecurity skills ecosystem. If the consortium sustains coordination, updates and reuses its assets strategically, and connects exploitation efforts to emerging educational, professional, and innovation needs, the project's results can continue to generate value well beyond the formal project duration.