Deliverable D3.6

Platform Concept and Course Format Offering – Intermediate Version

Contractual Date:	**30.04.2026**
Actual Date:	**27/04/2026**
Grant Agreement No.:	**101189986**
Work Package:	**WP3**
Lead Partner:	**Polytechnic University of Milan**
Authors:	Lorenzo Binosi (Polytechnic University of Milan)
Contributors:	28DIGITAL, Talent Garden Italia, Riga Technical University, Lusófona University

Versioning and contribution history

Version	Date	Author/s	Notes
0.1	10/04/2026	(Lorenzo Binosi) Polytechnic University of Milan	
0.2	27/04/2026	(Lorenzo Binosi) Polytechnic University of Milan	

Partner review table

Version	Reviewer (Partner)	Date	Scope of review	Action taken in document
0.1	Talent Garden Italia	11/04/2026	Review of the draft	Feedback incorporated
0.1	Tampere University	13/04/2026	Review of the draft	Feedback incorporated
0.1	28DIGITAL	16/04/2026	Review of the draft	Feedback incorporated
0.1	Lusófona University	27/04/2026	Review of the draft	Feedback incorporated

Executive summary

This deliverable, D3.6 — "CYCERONE Platform Concept and Course Format Offering (Intermediate Version)", as defined in the Grant Agreement, presents the intermediate design of the educational architecture developed by the CYCERONE project at month 16 of its 36-month cycle. CYCERONE is a European project funded under the EU's DIGITAL Europe Programme that addresses the cybersecurity skills gap identified by the European Cybersecurity Skills Academy initiative, with the goal of delivering a unified, role-oriented, and competence-driven training offering to Small and Medium-sized Enterprises and public administration professionals across the Union.

The deliverable describes how the CYCERONE training offering is shaped, rather than what it contains: the specific course catalogue is documented in the companion deliverable D4.5. It establishes a terminology framework aligned with the ENISA European Cybersecurity Skills Framework and the European e-Competence Framework; defines a common course schema covering provider, language, audience, level, duration, delivery format, and the Skills, Knowledge, and e-Competences addressed; introduces a three-pillar educational architecture (Awareness, Foundations, Hands-On) supported by a competence-driven Learning Path design; sets out the collaborative model for course curation, sharing, translation, and multi-partner delivery; and presents the conceptual design of the CYCERONE Education Portal as the digital entry point through which trainees discover the offering and follow their personal learning journey.

As an intermediate deliverable, D3.6 is a design document: it defines the structural and pedagogical framework on which the catalogue will be built, and the portal (previously planned as platform) will be implemented. The final version (D3.1, due at M36) will complement this design with evidence from actual course delivery, quality assurance feedback, and the lessons learned during the second half of the project.

List of contents

List of figures

1. Introduction

Cybersecurity has become one of the most critical and fastest-growing professional domains in the European Union. The accelerating pace of digital transformation, the rising frequency and sophistication of cyber threats, and the entry into force of regulatory frameworks such as NIS2 [8], GDPR [9], the Cyber Resilience Act [13], and the AI Act [12] have created an unprecedented demand for cybersecurity professionals across all sectors of the economy. This demand is felt most acutely by Small and Medium-sized Enterprises (SMEs) and public administration bodies, which often lack the in-house expertise and the structured training pathways available to larger organisations [18]. Bridging this skills gap is recognised at the European level as a strategic priority, most visibly through the European Cybersecurity Skills Academy initiative launched by the European Commission in 2023.

CYCERONE (*CYbersecurity aCadEmy foR educatiOn and experieNcE*) [17] is a European project for cybersecurity education and professional development that responds directly to this challenge. Funded under the EU's DIGITAL Programme, CYCERONE brings together a consortium of 16 organisations from 10 EU countries, including 11 higher education institutions. Over a 36-month project cycle, the consortium designs, harmonises, and delivers a unified cybersecurity training offering targeting SMEs and public administration professionals across the Union, with a strong emphasis on practical, role-oriented, and competence-driven learning.

This deliverable, D3.6, is the intermediate version of the "*CYCERONE platform concept and course format offering"*, fulfilling the requirements of Task 3.1 — *"Design of the education programmes, modules and units' format"*. As defined in the Grant Agreement, the goal of T3.1 is to design the portal-based offering in terms of structure and format definition for the foreseen programmes, courses, modules, and units.

To better reflect the currently intended purpose, the consortium has decided to use the term CYCERONE "portal" instead of "platform," as referred to in the Grant Agreement. In various titles of deliverables cited in this report, it is still defined as "platform" solely to maintain formal consistency with the original plan. The term "portal" more accurately conveys the system's informational and navigational functions, distinguishing it from content-hosting or learning management solutions.

D3.6 describes the form of the offering in the adopted portal, how courses are structured into modules and units, how they are delivered, how the consortium collaborates to produce and maintain them, how the CYCERONE Education Portal enables their discovery, and how learning paths guide trainees toward specific professional roles. It does not describe the content of the offering: the specific list of courses, their syllabi, their partner assignments, and their content descriptions are presented in the companion deliverable D4.5 (CYCERONE List of Courses and Associated Contents — Intermediate Version) [20], which is released in parallel.

A core methodological choice supporting this deliverable is the alignment with established European reference frameworks. The CYCERONE terminology, role definitions, and competence vocabulary are derived from the ENISA European Cybersecurity Skills Framework (ECSF) [1] and the European e-Competence Framework (e-CF) [3]. This grounding ensures that the CYCERONE offering is interoperable with other European cybersecurity education initiatives, recognisable to employers and trainees across Member States, and ready for integration into broader EU ecosystems such as the European Cybersecurity Skills Academy [5] and other planned, future opportunities [22].

1.1 Methodology

The portal concept and format design presented in this document was developed through a structured process involving all consortium partners:

- **M1–M4:** Collection and mapping of each partner's existing cybersecurity course catalogue, delivery infrastructure, and pedagogical capabilities. This stage produced an inventory of more than one hundred existing courses across the consortium, providing the empirical baseline for the harmonisation effort.

- **M5–M8:** Development of the classification framework, terminology, and format typology through alignment workshops with all partners. The terminology was iteratively refined to align with ECSF and e-CF vocabulary, ensuring European interoperability.

- **M9–M12:** Integration of findings from the D4.4 Skills Gap Report [18], including the most critically valued cybersecurity competences, the preferred delivery formats and learning modalities, and the priority professional roles for SME and public administration audiences.

- **M1–M14:** Definition of the portal governance framework and operational model under Task T3.2.

1.2 Relationship with Other Deliverables

This deliverable is closely connected to several other project outputs:

- **D4.5 (CYCERONE List of Courses and Associated Contents — Intermediate Version [20], Polytechnic University of Milan, M16):** The companion deliverable presenting the specific course catalogue with content descriptions, partner assignments, and learning path options. D3.6 defines the framework; D4.5 populates it.

- **D4.4 (Skills Gap Report — Intermediate Version [18], Riga Technical University, M16):** Provides the empirical foundation for the format design, identifying the most critically valued cybersecurity competencies and preferred learning formats.

- **D3.2 (CYCERONE Platform Governance and Operational Model [19], 28DIGITAL, M14):** Defines how the portal is governed and operated, informing the format design constraints.

- **D3.1 (CYCERONE Platform Concept and Course Format Offering — Final Version, Polytechnic University of Milan, M36):** The final version of this document, incorporating lessons learned from actual course delivery and continuous updates.

- **D3.4 (Digital Platform and User Manual, 28DIGITAL, M36):** The actual portal implementation described in Section 5.

1.3 Structure of This Document

The remainder of this document is organised to guide the reader from the conceptual foundations to the operational components of the CYCERONE offering.

Section 2 establishes the terminology framework, including the alignment with European reference frameworks (ECSF, e-CF) and the CYCERONE-specific concepts that underpin the rest of the deliverable.

Section 3 presents *what is offered*: the organisation of the CYCERONE training offering, the common attributes of every course, the supported delivery formats, the three-pillar architecture, and the design of learning paths.

Section 4 describes *how the offering is produced*: the collaborative model that underpins course curation, sharing, and translation across the consortium.

Section 5 describes *how the offering reaches trainees*: the CYCERONE Education Portal as the central entry point for course discovery, lead generation, and partner integration.

Section 6 concludes the deliverable with a synthesis of the work to date and a forward look toward the final version (D3.1) at M36.

2. Definitions and Terminology

A consistent terminology framework is essential for ensuring coherence across the CYCERONE consortium and for guaranteeing interoperability with the broader European cybersecurity education ecosystem. To this end, CYCERONE adopts and aligns its terminology with established European standards: the ENISA European Cybersecurity Skills Framework (ECSF) [1, 2], which defines professional Role profiles and their associated Skills, Knowledge Areas, and Tasks; the European e-Competence Framework (e-CF) [3], which provides the standard vocabulary of e-Competences and proficiency levels used across the EU ICT sector.

By aligning its definitions with these frameworks, CYCERONE ensures that its training offering is directly interoperable with ENISA role profiles, comparable across EU Member States, and recognisable to employers and trainees throughout the Union. This section establishes the standard definitions used throughout the project, building on these European references while introducing CYCERONE-specific concepts where needed. These definitions apply uniformly across all project deliverables and partner communications.

2.1 European Reference Frameworks

CYCERONE aligns with two established European frameworks that provide the standard vocabulary for cybersecurity education and professional competence across the European Union:

- **European e-Competence Framework (e-CF) [3].** The e-CF is a European standard that defines forty-one e-Competences grouped into five areas (Plan, Build, Run, Enable, Manage), each specified at up to five proficiency levels. The e-CF provides the common vocabulary used by ICT professionals, employers, and education providers across the EU.

- **ENISA European Cybersecurity Skills Framework (ECSF) [1].** Published by the European Union Agency for Cybersecurity, the ECSF defines twelve professional Role profiles covering the cybersecurity workforce (such as Chief Information Security Officer, Incident Responder, Penetration Tester, and Cyber Threat Intelligence Specialist). Each Role profile specifies the associated Tasks, Key Skills, Key Knowledge, e-Competences, and typical Deliverables.

2.2 CYCERONE Terminology

The CYCERONE portal introduces a small set of project-specific terms that build on the European reference frameworks above. The following definitions apply throughout this document and all companion deliverables:

- **Resource.** The smallest, atomic, indivisible building block of the CYCERONE educational offering. A Resource is a single, self-contained learning artefact such as a document, presentation, video, virtual machine, lab environment, or assessment tool.

- **Unit.** An indivisible collection of Resources that must be consumed together to convey their intended learning value. A Unit is composed of one or more Resources whose individual usefulness is limited outside the context of the Unit — for example, a video lecture paired with the quiz that assesses it, or a tutorial document accompanied by the lab environment it walks the trainee through.

- **Training Module.** A structured collection of Units organised in a specific order, designed to teach specific Skills and Knowledge and to target a specific e-Competence at a given proficiency level. Training Modules are independently valuable: a trainee who completes a single Training Module gains a meaningful, self-contained competency.

- **Course.** A coherent aggregation of Training Modules that develops one or more Skills, Knowledge, and e-Competences. Courses represent the primary deliverable unit within the CYCERONE project. The full list of courses and their contents is presented in the companion deliverable D4.5.

- **Learning Path.** An ordered collection of Courses designed to guide a trainee toward acquiring the Skills, Knowledge, and e-Competences required for a specific target Role.

- **Pillar.** One of three overarching categories — Awareness, Foundations, and Hands-On — that organise the CYCERONE training offering by depth and pedagogical approach. Each Course belongs to exactly one Pillar. The three Pillars are described in detail in Section 3.

- **Tier.** A subdivision of the Foundations Pillar that groups Courses by audience and pedagogical purpose.

2.3 Mapping to University Terminology

The following mapping relates CYCERONE terminology to standard university structures:

- Programme / Degree → Learning Path

- Course → Course

- Course Module → Training Module

- Teaching Resources (textbooks, readings, presentations, videos, assignments, assessments, labs, discussion forums) → Resources

This mapping enables partner universities to translate their existing academic offerings into the CYCERONE framework without ambiguity.

2.4 Relationship Between Concepts

The CYCERONE architecture follows a competence-driven model: Roles require Skills, Knowledge, and e-Competences, which can be acquired through Training Modules composed of Resources. Training Modules are grouped into Courses, and Courses are sequenced into Learning Paths that target specific Roles. Figure 1 illustrates the relationships between these core elements. Within the CYCERONE portal Courses are further organised into Pillars. This layered architecture ensures that the offering can be consumed at multiple granularities — from a single Resource for targeted reference, to a full Learning Path for comprehensive professional development.

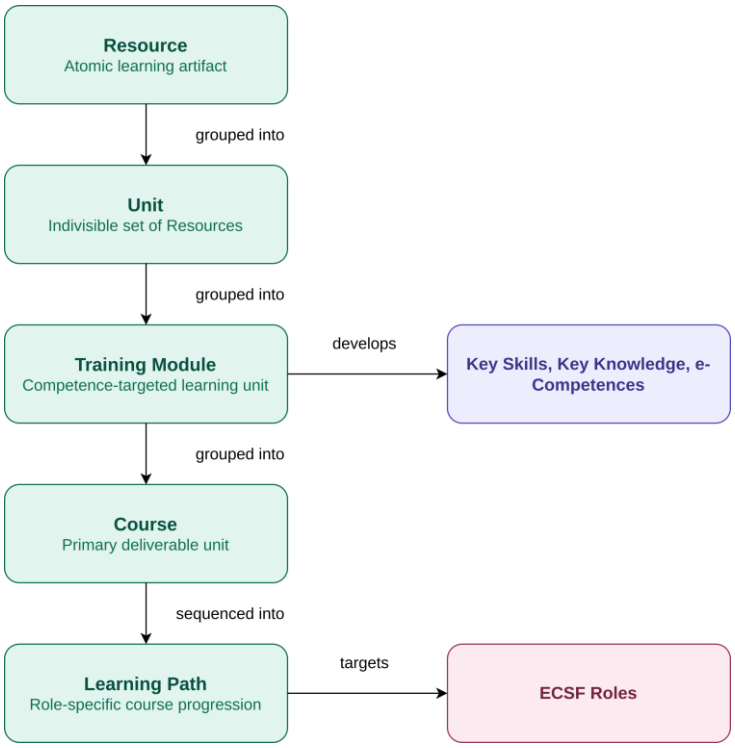

Figure 1: The CYCERONE concept model.

3. Organisation of the CYCERONE Training Offering

This section explains how the CYCERONE training offering is structured. It first outlines the common attributes shared by all Courses on the portal, then describes the delivery formats the portal supports. It next presents the three-pillar architecture that organises the full course offering and finally explains how Learning Paths cut across this architecture. The specific courses populating the offering, along with their concrete attribute values, are documented in the companion deliverable D4.5.

3.1 Course Characteristics

Every Course in the CYCERONE offering is described by a common set of attributes. These attributes form the schema of the catalogue:

- **Provider(s).** The consortium partner(s) responsible for delivering the course.
- **Language.** The language or languages in which the course is offered. Courses are produced in English and may be translated into partner languages for local delivery; the language policy is described in Section 4.
- **Key Skills.** The Skills from the ECSF Role profiles that the course develops.
- **Key Knowledge.** The Knowledge areas from the ECSF Role profiles that the course addresses.
- **Level.** The depth of the course content, expressed as one of: beginner, intermediate, advanced, or mixed. This attribute is distinct from the Pillar: while the Pillar reflects the course's pedagogical role within the CYCERONE architecture (Section 3.3), the Level reflects the depth of content relative to the learner's prior knowledge.
- **Target audience.** The professional profiles the course is intended for (for example: manager, CTO, developer, security analyst). The target audience may correspond directly to one or more ECSF Roles (e.g., Penetration Tester, Cybersecurity Implementer) or to broader SME and public-administration

professional figures that combine responsibilities across several Roles.

- **Duration.** The total length of the course, expressed in hours, days, weeks, or calendar time, depending on the delivery format.
- **Estimated effort.** The expected learner workload to complete the Course, expressed in hours and split into contact hours (interaction with an instructor or peers under instructor guidance, e.g. live sessions, workshops, supervised labs) and non-contact hours (independent activity, e.g. recorded lectures, readings, exercises, project work). Total effort is the sum of the two.
- **Format.** The delivery modality, chosen from the options described in Section 3.2: online, in-person, or hybrid. Depending on the format, additional attributes apply:
    - *If in-person or hybrid:* **Location** — the venue where the in-person component takes place.
    - *If online:* **Live or on demand** — whether the course is delivered in scheduled live sessions (synchronous) or made available for self-paced consumption (asynchronous).
    - *If in-person:* **Availability** — the scheduled dates or windows during which the course is offered.

Moreover, Training Modules and Resources are characterised by a smaller set of attributes: each Training Module specifies the e-Competence it targets, its proficiency level, the ordered sequence of Resources that compose it, and its associated assessment tool; each Resource specifies its type and its version. The versioning of Resources supports life-long auditing and allows Training Modules and Courses to be updated over time without losing traceability of the learning artefacts consumed by each trainee.

3.2 Delivery Formats and Modalities

The CYCERONE training offering supports multiple delivery formats to accommodate the diverse needs and constraints of professionals in SMEs and public administration. The choice of delivery format for each course is left to the organisation delivering the course, according to its infrastructure, capacity, and target audience.

3.2.1 Online Asynchronous

Online asynchronous delivery allows trainees to access course materials, lectures, and assessments at their own pace and schedule. This format is particularly suited to professionals in SMEs who cannot easily be released from their duties for extended periods.

Characteristics: self-paced progression, pre-recorded video lectures, downloadable readings and exercises, automated assessments, discussion forums for peer interaction, no requirement for simultaneous attendance.

3.2.2 Online Synchronous

Online synchronous delivery involves scheduled, real-time sessions conducted via video conferencing platforms. This format enables direct interaction between instructors and trainees, group discussions, and live demonstrations — while still eliminating the need for physical travel, making it accessible across EU Member States.

Characteristics: scheduled live sessions, real-time instructor-trainee interaction, live demonstrations and Q&A, group exercises and breakout rooms, screen sharing for tool demonstrations.

3.2.3 Face-to-Face

Face-to-face delivery involves in-person instruction at a partner university or designated training venue. This format is most appropriate for courses that require physical access to specialised equipment, intensive hands-on workshops, or on-site team exercises.

Characteristics: physical presence required, access to specialised laboratory equipment, intensive workshop-style interaction, networking opportunities among trainees, typically delivered in concentrated blocks.

3.2.4 Blended

Blended delivery combines online and in-person elements within the same course, offering the flexibility of remote access for theoretical content alongside the engagement of face-to-face interaction for practical exercises. In a typical blended course, theoretical Training Modules are delivered asynchronously online, while practical laboratories, tool workshops, and assessment sessions are conducted synchronously — either in person at a partner venue or via live online sessions.

Characteristics: combination of asynchronous theoretical content and synchronous practical sessions, flexibility for trainees who cannot commit to full-time in-person attendance, strong alignment with the blended-learning preference expressed by D4.4 survey respondents.

3.2.5 Format Selection Criteria

The choice of delivery format to each course follows a set of ordered criteria developed in consultation with all consortium partners:

1. **Partner infrastructure:** The delivery format must be compatible with each partner's existing teaching infrastructure and platform capabilities.

2. **Target audience accessibility:** Courses targeting SME professionals across multiple EU countries should prioritize online or blended formats to minimise travel barriers.

3. **D4.4 survey preferences:** The format selection reflects the expressed preferences of the target audience, with blended learning as the default where feasible.

4. **Content type:** Theoretical and conceptual content is suited to online asynchronous delivery; tool-based practical content requires synchronous or face-to-face interaction.

5. **Course duration:** Short courses (under 20 hours) are well-suited to fully online delivery; longer courses benefit from blended approaches.

3.3 The Three-Pillars Architecture

The CYCERONE training offering is organised around three pillars that represent increasing depth and specialisation. The architecture is designed to serve the full range of CYCERONE's target audiences, from non-technical professionals who need basic cybersecurity literacy through to IT specialists who require hands-on expertise with industry-standard tools.

The three-pillar model directly responds to the findings of D4.4 (Skills Gap Report, Intermediate Version) [18], which identified a persistent theory-to-practice divide as the most significant challenge in cybersecurity education. By separating conceptual awareness from professional foundations and practical application, the architecture ensures that each pillar serves a distinct pedagogical purpose, with each level building upon the previous one without prescribing a mandatory sequence: Courses in each Pillar are self-contained and can be taken independently, allowing trainees to combine them according to their prior knowledge and professional objectives.

3.3.1 Pillar 1: Awareness

The Awareness pillar comprises short, accessible courses for all professionals, regardless of technical background. They build foundational cybersecurity literacy and are suitable for employees at any level within SMEs and public administration bodies. These courses are practical and relevant to everyday professional activities, with no technical prerequisites and a focus on recognition and prevention rather than technical implementation.

The majority of CYCERONE trainees are not pursuing a career as cybersecurity specialists, but they still need to operate safely within an increasingly digitalised work environment. For these trainees, Awareness courses can constitute the entire training journey, taken on their own without progressing into the next Pillars.

3.3.2 Pillar 2: Foundations

The Foundations pillar comprises professional-depth courses that provide the core Skills, Knowledge, and e-Competences required for specific ECSF Roles [1]. Each Foundations course is mapped to one or more Role profiles and addresses the e-Competences that those profiles require at the relevant proficiency levels. Foundations courses go significantly beyond the Awareness level in both depth and duration, and they integrate open-source tool training directly into the curriculum, in line with the D4.4 finding that a majority of respondents identified the lack of hands-on experience as the most significant shortcoming in cybersecurity graduates [18].

The Foundations pillar is the largest of the three and is internally organised into four Tiers, each addressing a distinct audience within the broader population of cybersecurity practitioners and adjacent professionals:

- **Tier 1 (For All Audiences)** extends Awareness content into more structured offerings that remain accessible to every professional, without requiring a technical or management specialisation. Tier 1 serves trainees who want to deepen their understanding of cybersecurity beyond literacy level without committing to a specific Role.

- **Tier 2 (Technical Foundations)** addresses the technical ECSF Roles, with an emphasis on laboratory-based content and tool training. Tier 2 serves trainees who are building the technical competences associated with operational cybersecurity Roles such as Cybersecurity Implementer, Penetration Tester, Cyber Incident Responder, Digital Forensics Investigator, Cybersecurity Architect, and Cyber Threat Intelligence Specialist.

- **Tier 3 (Management and Governance)** addresses the strategic, organisational, and compliance dimensions of cybersecurity. Tier 3 serves trainees in or moving towards governance Roles such as CISO, Cybersecurity Risk Manager, Cybersecurity Auditor, and Cyber Legal, Policy and Compliance Officer.

- **Tier 4 (Transversal Specialisations)** covers topics that several ECSF Roles apply in their work regardless of their specialisation, such as applied cryptography, threat modelling, AI security, and software supply chain security. Tier 4 serves trainees who, regardless of their primary Role, need depth in a topic that spans technical and management boundaries.

Tiers apply only within the Foundations pillar; the Awareness and Hands-on pillars are not subdivided.

3.3.3 Pillar 3: Hands-On

The Hands-On pillar comprises Hackathons, Capture-the-Flag (CTF), and simulation-based courses. These courses are designed as the culminating experience of the CYCERONE learning journey: trainees apply the tools and knowledge acquired in the Foundations pillar to realistic, scenario-based challenges.

Consequently, some Roles — such as Chief Information Security Officer (CISO) or other governance- and

management-oriented profiles — will not include Hands-On courses in their Learning Paths, as their professional responsibilities focus on strategy, policy, and oversight rather than direct technical execution. For these Roles, the Learning Path is completed at the Foundations level.

3.4 Learning Paths Design

Learning Paths traverse the three-pillar architecture to guide trainees from foundational literacy to practical mastery for a specific target Role. A typical Learning Path begins with a selection of Awareness courses, progresses through the Foundations courses, and culminates in one or more Hands-On courses where the acquired tools and knowledge are applied to realistic scenarios. Learning Paths are recommended journeys rather than rigid prescriptions: depending on their prior knowledge and professional needs, trainees may follow a Learning Path in full or select only the courses relevant to them, entering and exiting the path at different points.

The design of a Learning Path is driven by the Skills, Knowledge, and e-Competences associated with the target Role [1, 2, 4]. As described in Section 3.1, every Course in the CYCERONE catalogue declares the Key Skills, Key Knowledge, and e-Competences it develops. Constructing a Learning Path therefore reduces to a matching problem: starting from the Role profile defined by the ECSF, the design selects all the Courses whose declared Skills, Knowledge, or e-Competences contribute to the requirements of that Role. The selected Courses are then ordered first by Pillar (Awareness → Foundations → Hands-On) and, within each Pillar, by Level (beginner, intermediate, advanced).

To illustrate the principle, consider the Penetration Tester Role, which according to the ECSF requires Key Skills such as:

- Develop codes, scripts, and programmes
- Perform social engineering
- Identify and exploit vulnerabilities
- Conduct ethical hacking

Suppose three Courses in the CYCERONE catalogue declare the following Skills:

- **Course A** develops "Develop codes, scripts, and programmes."
- **Course B** develops "Identify and exploit vulnerabilities" and "Conduct ethical hacking."
- **Course C** develops "Perform social engineering."

All three Courses contribute to the Penetration Tester Role and are therefore selected for the Learning Path. The ordering follows the Pillar–Level rule: if Course C belongs to the Awareness pillar, and Courses A and B are Foundations courses at beginner and intermediate level respectively, the resulting Learning Path is **C → A → B**. A trainee following this path first acquires baseline awareness of social engineering, then learns to develop scripts and tools, and finally progresses to vulnerability identification and ethical hacking practice.

This example shows how the competence-driven model introduced in Section 2 translates into a concrete pathway: the ECSF Role defines the requirements, the Courses declare what they offer, and the Pillar–Level ordering provides the pedagogical sequence. The same procedure applies to any Role for which the consortium offers a Learning Path.

It should be noted that the CYCERONE catalogue cannot exhaustively cover every single Key Skill, Key Knowledge

area, and e-Competence associated with every ECSF Role. With a target of 36 courses across the consortium, and with the breadth of the ECSF Role profiles, full coverage is not in scope for the project. The Learning Paths are designed to address the most critical and most frequently demanded competences for each target Role, as identified in the D4.4 Skills Gap Report [18], while acknowledging that some specialised or peripheral requirements will remain outside the catalogue. This is a deliberate design choice: the goal of CYCERONE is to provide focused, high-impact training journeys aligned with market demand, rather than to replicate the full curriculum of a multi-year academic programme.

4. Course Curation and Co-Creation

The CYCERONE training offering is the result of a collaborative effort across 11 partner universities and the broader consortium. While each course is curated by a single responsible partner, the model explicitly supports cross-partner contribution, reuse of learning artefacts, and partner-led translation into local languages. This section describes the governance and language model that underpins course development across the consortium.

4.1 The Curator Role

Every Course in the CYCERONE catalogue has a single curator, a designated partner organisation that holds primary responsibility for the course throughout its life cycle. The curator is responsible for:

- Defining the course syllabus and the sequence of Training Modules.
- Ensuring that the course addresses the Skills, Knowledge and e-Competences declared in its metadata.
- Maintaining the course over time, including content updates and quality improvements.
- Evaluating Resources and Training Modules shared by other partners for possible inclusion in the course.

Single curatorship ensures clear accountability and avoids the coordination overhead that would arise from shared responsibility across multiple institutions. At the same time, it does not preclude collaborative content development, as described in the next subsection.

4.2 Sharing and Reuse of Resources and Training Modules

To support cross-partner reuse and avoid duplication of effort across the consortium, partners are expected to make their Training Modules and Resources available to the consortium as they are produced. Together, these contributions form a common pool of learning artefacts from which any curator can draw when designing a new Course.

This sharing model serves two purposes.

First, it reduces duplication of effort: a Training Module on, for example, network traffic analysis developed by one partner can be reused by other curators rather than re-created from scratch.

Second, it allows each Course to benefit from the specific expertise of multiple institutions, since a curator can assemble a Course by combining their own materials with high-quality contributions from other partners.

In practice, sharing and reuse work as follows:

- **Sharing.** Partners share their Training Modules and Resources with the consortium as soon as they are ready, together with the metadata that describes them (description, e-Competence targeted, proficiency level, Skills and Knowledge addressed, language, version). This metadata enables curators to discover and assess reusable content.

- **Discovery and evaluation.** When designing a Course, the curator reviews the shared pool to identify Training Modules and Resources that match the Course's intended Skills, Knowledge, and e-Competences. The curator decides whether each candidate artefact is suitable for inclusion in the specific pedagogical context of the Course.

- **Attribution.** Contributing partners are credited as authors of the Training Modules and Resources they produce. When a curator incorporates an artefact from another partner, the contributing partner is credited in the Course metadata. The curator nonetheless retains overall responsibility for the Course in which the artefact is used.

- **Versioning.** As described in Section 3.1, every Resource is versioned. A Course always references a specific, identifiable version of every Resource it consumes, so that updates to a shared Resource by its original author do not silently propagate into Courses that depend on it. Curators can choose when and whether to adopt a newer version.

This model supports the modular architecture of the CYCERONE portal: the same Training Module can appear in multiple Courses curated by different partners, without duplication and without ambiguity about who is responsible for what. It also creates an incentive for partners to produce high-quality, reusable artefacts, since well-designed materials according to a robust set of standard ground rules for collaboration and designed as a shared asset can be adopted across the consortium.

4.3 Language Policy

To ensure consortium-wide accessibility and reusability, all Courses, Training Modules, and Resources must be created in English as the baseline language. English is the working language of the consortium and the *lingua franca* through which partners can review, reuse, and harmonise each other's contributions.

Beyond the English baseline, partners are free to translate courses into their own languages for delivery to local audiences. Localisation is voluntary: any partner that wishes to deliver a course in its own language may produce a translated version. The translated version is registered alongside the original in the catalogue and made discoverable through the CYCERONE Education Portal.

To maximise the reach of the offering across the European Union, a selected subset of asynchronous courses will be translated into multiple EU languages. Asynchronous courses are particularly well suited to wide-scale translation because their materials are stable, do not depend on live instructor delivery, and can be consumed independently of language-specific support. This effort directly supports the CYCERONE objective of making cybersecurity training accessible to SMEs and public administration professionals across all Member States, regardless of their working language.

This approach balances two competing goals: ensuring that the entire offering is accessible in a common language for reviewers, employers, and trainees across the EU, while also enabling partners to serve their national audiences in the language those audiences prefer.

4.4 Delivery by Multiple Partners

A Course curated by one partner may also be delivered by other partners. This typically occurs when a partner wishes to offer the Course in its own language, when multiple partners want to deliver the same Course in parallel to different audiences, or when a partner delivers it to its national network of SMEs and public administrations. In all cases, the curator and the original contributing partners are credited in the local delivery materials.

When delivering a Course, partners may tailor its content to reflect the local context — for example, by referencing national legislation and regulatory frameworks, citing examples relevant to the local SME and public administration landscape, or emphasising aspects of the syllabus that match the needs of the specific target group.

Delivery by a partner other than the curator does not transfer curatorship: the curator remains responsible for the Course content as defined in the catalogue, and the delivering partner is responsible for the local delivery experience (scheduling, instructor assignment, language adaptation, and trainee support).

5. The CYCERONE Education Portal

The CYCERONE Education Portal constitutes the central entry point to the consortium's training offering. The portal delivers a consistent and low-friction user journey across heterogeneous partner environments, while preserving a clear operational boundary: course delivery and enrolment fulfilment remain on the respective partner platforms, while the portal focuses on discovery, lead generation, and training offering publication. In line with the governance and operational model defined in Deliverable D3.2, the portal functions as a lightweight, shared interface that enhances the visibility and discoverability of cybersecurity training offerings from consortium partners.

5.1 Mission, Scope and Features

The CYCERONE Education Portal serves as the single, unified entry point to the consortium's training offering. Through the portal, users can discover cybersecurity courses showcased centrally from across the consortium, create a personal account, receive personalized course suggestions based on their profile and needs, register for courses, or request additional information from the relevant course provider. When a user expresses interest in a course, the portal redirects them to the respective partner's website or learning environment for registration and participation in educational activities.

The portal implementation encompasses three core components: Portal Implementation and Management, Seamless Navigation and User Experience Design, and Integration with the CYCERONE Website.

A strict separation of concerns applies: the portal manages discovery and lead generation only, while course delivery, enrolment fulfilment, and learner management remain entirely on partner platforms. The portal does not host or deliver courses, nor does it store course videos, files, or assignments. All learning content resides on partner systems. This architecture respects the heterogeneity of partner environments and avoids the technical and governance complexity of a centralized delivery system.

The portal provides the following features:

- **Unified Course Catalogue**: a governed taxonomy with standardised course factsheets enabling cross-partner comparison and consistent filtering (see Section 5.4).

- **User Account and Profiling**: a lightweight account-creation process that enables personalized interactions with the catalogue (see Section 5.3).
- **Learning Pathways**: rule-based course recommendations driven by the user's competence level and professional objectives, extensible to dynamic AI-driven logic in a future phase (see Section 5.5).
- **Lead and Registration Management**: dual conversion pathways ("Contact Me" and "Register Now") with structured data transmission to the responsible course provider (see Section 5.6).
- **Partner Curator Dashboard**: a back-office interface enabling partners to manage their catalogue entries, update course metadata, and monitor lead flow.
- **Responsive and Multilingual Interface**: baseline coverage in English plus partner languages, with architecture accommodating an AI Translation Plugin for additional EU languages.
- **Privacy-by-Design**: anonymous analytics for discovery, with personal data collected only upon explicit user consent.

5.2 User Journey

The user journey through the portal follows four stages, with a clear handoff between portal and partner responsibilities.

- **Step 1 — Discover and Search (Portal responsibility)**: Users browse the unified course catalogue (see Section 5.4) freely, without the need for registration. Filters by topic, format, level, and language are available to identify relevant training offerings. During this phase, only anonymous usage data is collected.
- **Step 2 — Account Creation (Portal responsibility)**: When a user identifies a course of interest and wishes to take action — either requesting more information or registering — the portal requires the creation of a personal account. The user provides basic profile information (name, email, organisation, country, role, cybersecurity knowledge level), which also enables personalized course recommendations for future visits (see Section 5.3).
- **Step 3 — Evaluate and Engage (Portal responsibility)**: Once registered, users compare course factsheets featuring standardised objectives, providers, and formats. Two conversion pathways are available: "Contact Me" for lead generation and "Register Now" for enrolment initiation. The mechanics of these pathways are described in detail in Section 5.6.
- **Step 4 — Partner Handoff (Partner responsibility)**: The portal transmits the user's data to the relevant partner (subject to explicit user consent) and redirects the learner to the partner's platform for enrolment confirmation, course delivery, and all subsequent communication.

Data ownership transitions across these stages. During discovery (Step 1), only anonymous usage data (page views, click counts) is collected and remains under portal-level ownership. From account creation onward (Steps 2–3), identifiable leads and registrations are captured and managed at the portal level. Once the handoff occurs (Step 4), enrolment records, training progress, attendance, grades, and certificates fall under the full ownership and responsibility of the respective partner organisation. The data governance framework is described in Section 5.8.

5.3 User Account and Profile Management

The portal supports the creation of individual user accounts, enabling personalized interactions with the training catalogue. During account creation, users provide basic profile information including their name, email address, organisation, country, professional role, years of experience, and an indication of their current cybersecurity knowledge level. This profiling data serves two purposes: it enables the portal to generate personalized course suggestions aligned with the user's background and objectives, and it supports aggregated reporting on participation patterns for project monitoring.

Once an account is created, the user gains access to the full course catalogue, personalized pathway recommendations (see Section 5.5), and the ability to register for courses or request further information from course providers. User account data is stored centrally within the CYCERONE system and managed exclusively at the portal administration level. Consortium partners do not have direct access to user profiles within the portal; they receive only the specific data necessary for the courses in which a user has expressed interest, and only upon the user's explicit consent.

Users retain full control over their account data at all times. Profile information can be updated or corrected, preferences can be modified, and account deletion can be requested in compliance with GDPR provisions. The regulatory framework governing user data is detailed in Section 5.8.

5.4 Course Catalogue and Metadata

The CYCERONE Course Catalogue is a comprehensive, unified listing of all courses offered within the project. Each course entry contains a standardised set of metadata fields, including the course title, a structured description, the consortium partner providing the course, available dates and scheduling information, delivery format (online, in-person, or blended), proficiency level (beginner, intermediate, advanced, or mixed), duration, target audience, and the specific cybersecurity competences addressed.

The catalogue aggregates training offers from across the consortium into a single, searchable interface with standardised course factsheets enabling cross-partner comparison and consistent filtering. Courses are hosted and delivered on each partner's own website or learning platform; the portal functions as the common entry point through which users discover and access the training offering.

The metadata model — covering course categories, topics, levels, formats, and language information — is collectively defined and maintained by the consortium through its Portal Working Group (PWG; see Section 5.9). The model may be refined during the project to improve consistency, usability, and interoperability with European-level platforms and underlying initiatives. Each consortium partner retains responsibility for keeping their course information accurate and up to date, including titles, descriptions, dates, session availability, capacity limitations, and any cancellations. The portal administration team manages the upload and publication of this information based on what partners provide, ensuring consistency in format, layout, and metadata standards.

5.5 Learning Pathways

The portal offers a pathway recommendation feature that guides users through the training catalogue based on their individual needs and profile. Users respond to a short set of questions regarding their current competence level, professional objectives, and desired skills. Based on these inputs, the portal suggests a recommended sequence of courses, indicating which offerings are most relevant, in what order they should be undertaken, and what competences the user will acquire upon completion.

The pathway logic is based on a set of rules defined in collaboration with the consortium and informed by the competence framework developed in WP4. At this stage, the system operates on deterministic rule-based matching rather than an advanced recommendation engine. The architecture is designed to be extensible,

allowing future evolution toward dynamic, AI-driven logic should the project or its successors require more sophisticated personalization capabilities. Consortium partners contribute to the pathway design by advising on how their courses should be tagged, grouped, and sequenced within the broader training offering.

5.6 Lead and Registration Management

When a user identifies a course of interest, the portal presents two distinct conversion pathways, each serving a different level of user commitment and triggering a different operational workflow.

The first pathway is the “Contact Me” option, which generates a lead. A lead represents a user who has expressed interest in a course but is not yet ready to commit to enrolment. The portal collects the user’s name, email address, the course of interest, and an optional message, and transmits this information to the relevant consortium partner. The partner then follows up directly with the user through their own communication channels (email, CRM, or other institutional tools). All leads are recorded in the portal’s administration dashboard to enable monitoring of partner responsiveness.

The second pathway is the “Register Now” option, which initiates a formal registration. The user selects a specific course and session date, confirms that their data may be shared with the delivering partner, and submits the registration form. The portal records the registration centrally and transmits the user’s details to the responsible partner. Registration on the CYCERONE portal constitutes a first step in the enrolment process; it does not automatically enrol the user into the partner’s LMS or course system. The partner retains full responsibility for confirming the participant’s place — particularly where courses have limited capacity — communicating with the participant, providing access to the learning environment, distributing pre-reading or course materials, sending reminders, and managing attendance throughout the course.

Once a lead or registration is generated, the data is transmitted to the partner through one of two mechanisms, depending on the partner’s technical readiness (see Section 5.7). For partners with advanced integration capabilities, transmission occurs automatically through a technical connection (API). For all other partners, the portal administration team exports leads and registrations in structured file formats (CSV or Excel) and distributes them at agreed intervals. Each partner designates a specific email address or system endpoint for receiving this data and acknowledges receipt.

5.7 Architecture and Integration

The portal operates on a two-directional model. On the input side, consortium partners provide their course information, which is then standardised according to the shared metadata framework described in Section 5.4. On the output side, when a user expresses interest in a course — either by requesting more information or by registering (see Section 5.6) — the portal transmits the relevant user data to the responsible course provider, subject to explicit user consent.

In addition to the inbound catalogue flow and the outbound lead and registration flow, the portal supports a return channel through which partners report back to the portal on the participation outcomes of users they have received. Once a user has been handed over to a partner platform for course delivery, the partner periodically reports to the portal a minimal set of status events — for example, enrolment confirmed, course in progress, course completed, or certificate issued — for the users who originated from the portal and who have given their consent for this feedback to be tracked. The portal records these status updates against the corresponding user profile, so that users can see in their personal area which courses they have completed across all consortium partners and download the associated certificates where available. This return channel transforms the portal from a one-way discovery interface into a unified personal dashboard that gives each trainee a consolidated view of their CYCERONE learning journey, regardless of how many partners delivered the courses they followed.

From a technical standpoint, the portal follows an API-First architecture built on open standards (OpenAPI 3.0 [15], React, Node.js) and hosted on cloud-native infrastructure (AWS). This design ensures that the portal can scale as the training catalogue grows and that it remains compatible with future EU-level platforms, including AKADIMOS future initiatives [22]. The modular architecture allows new features or integrations to be added without disrupting the existing system. Where technically feasible, metadata updates, participation data, and the return-channel status events described above are exchanged automatically between partner systems and the portal, reducing the need for manual data entry.

The integration approach follows a layered, capability-driven model designed to accommodate the different technical readiness levels of consortium partners. Mode 1 (Universal Baseline) relies on email and file-based exchange (CSV/Excel) and is mandatory for all partners, ensuring that every partner can participate regardless of their technical infrastructure. Mode 2 (Advanced Integration) provides system-to-system integration via APIs and/or LTI [16], activated only for partners that demonstrate readiness and complete technical onboarding. Both the inbound catalogue flow and the outbound return channel can operate at either mode: the same status events that an advanced partner reports through an API call can be reported by a baseline partner through a periodic CSV upload.

The portal also provides a Partner Curator Dashboard — a back-office interface enabling partners to manage their catalogue entries, update course metadata, monitor the flow of leads and registrations associated with their courses, and report participation status updates back to the portal. The Partner Curator Dashboard further hosts a shared workspace for didactic material, a dedicated area where partners can deposit, browse, and exchange Training Modules and Resources contributed to the consortium common pool described in Section 4.2. This shared workspace operationalises the sharing-and-reuse model defined at the governance level in Section 4: it provides the concrete digital space in which curators can publish their materials with the associated metadata, search and filter the contributions of other partners, and download artefacts for inclusion in the courses they curate. By integrating the shared workspace into the Partner Curator Dashboard, the portal ensures that course curation, catalogue management, and material reuse all happen within a single back-office environment.

5.8 Data Governance and Compliance

A clear delineation of data storage and protection responsibilities applies between the portal and partner systems. The CYCERONE portal centrally stores user account and profile data, the course catalogue, lead records, registration records (limited to the basic data submitted at the point of conversion), and user consent records. Partners, in turn, store within their own systems all data relating to course participants, attendance, grades, certificates, and all communication with participants during and after course delivery. They receive data only for the courses they deliver and only upon the user's explicit consent. In addition, the portal retains the minimal participation status events reported back by partners through the return channel described in Section 5.7 — for example, course enrolment, completion, and certification status — associated with the corresponding user profile and limited to users who have explicitly consented to this consolidated tracking. Grades, attendance records, and other detailed participation data are not stored centrally and remain on partner systems.

The CYCERONE portal operates as the Data Controller for user accounts and for the data collected during the discovery and selection phases. Once a user's data is forwarded to a partner in the context of a specific course registration or lead, the partner assumes the role of Data Controller for their part of the training process. Partners are bound to use the received data exclusively for the purpose of delivering the training, unless additional consent is obtained. Should a user request data correction or deletion, both the portal and the relevant partner must cooperate to fulfil the request across all systems involved.

Personal data processing across the portal follows well-established EU project-wide GDPR practices, including data minimisation, purpose limitation, and secure data handling. All users who create an account are informed, through transparent privacy notices made available at the point of registration, about how their personal data is

collected, stored, processed, and retained. Participants are also informed of their rights under the GDPR, including the rights of access, rectification, and deletion.

Beyond GDPR, the compliance framework adheres to the transparency and data accessibility principles set out in the Digital Services Act (DSA) [10] and the EU Data Act [11], ensuring that publicly available training information remains accurate, traceable, and interoperable. While no AI-based functionalities are currently implemented, the design principles support future compliance with the EU AI Act [12] standards for trustworthy digital services. Accessibility follows the WCAG 2.1 standard [14], promoting equitable access to training opportunities across Member States, and the portal makes course information available in multiple EU languages — with baseline coverage in English plus partner languages, and an architecture that accommodates an AI Translation Plugin for additional EU languages.

5.9 Governance Framework

The governance and operational model for the CYCERONE portal, as defined in Deliverable D3.2, ensures coordination, shared ownership, and transparent decision-making throughout the project lifecycle. The governance approach follows a lightweight, streamlined design that avoids unnecessary committees or administrative layers, relying instead on the existing Project Executive Committee (PEC) and WP3 coordination structures.

During the project phases, the CYCERONE portal is jointly owned by all consortium partners as a shared asset. The governance structure operates through three layers. The PEC serves as the primary strategic oversight and decision-making body, approving significant changes and ensuring continued alignment with the overall project objectives. Decision-making within the PEC follows a qualified majority rule, requiring a two-thirds majority of the votes. The Portal Working Group (PWG) operates under the authority of the PEC as the primary coordination forum for operational and implementation matters, bringing together the defined portal governance roles across technical, content, quality, communication, and partner-level coordination functions. Where required, a Technical Subgroup (TS) may be established under the PWG domain to focus on technical solutions, interfaces, and data flows across the consortium.

The governance model incorporates provisions for future alignment with European-level cybersecurity skills initiatives. The “plug-in” model enables the CYCERONE portal to integrate into larger EU ecosystems without redesign, ensuring continuous relevance and sustainability beyond the project’s duration. A detailed description of the governance structure, roles, and decision-making processes is provided in Deliverable D3.2.

5.10 Content Lifecycle and Quality Assurance

The content lifecycle management for the CYCERONE portal encompasses the full process from initial submission to ongoing maintenance. The initial creation and definition of training courses to be featured on the portal are coordinated under Work Package 4 (WP4), which develops education programmes, modules, and learning units in line with the project objectives and agreed quality principles.

Once the portal is operational, the approval of new courses and updates to existing courses follows a structured workflow managed through interactions between WP4 and the PWG. Quality-related checks focus on compliance with agreed criteria, metadata standards (see Section 5.4), and overall compliance requirements. Responsibility for pedagogical input to content and course delivery remains with the respective curator within each partner institution. The portal and its governing body ensure that the presentation and availability of all listed courses meet consistent, effective criteria.

To ensure ongoing relevance and quality, a feedback and continuous improvement mechanism is in place.

Partners provide feedback on usability, data accuracy, and content needs via WP3 coordination meetings. Periodic reviews are conducted by WP3 and the PWG with the portal administrator to evaluate performance using established indicators (e.g., number of visits, clicks, and partner updates) and assess the need for improvements. Lessons learned arising from these reviews are integrated into subsequent updates, ensuring continuous optimisation of portal functionality, visibility, and user experience.

5.11 Portal Lifecycle and Sustainability

The portal lifecycle is structured across three phases. The Design and Development phase (M1–M18) covers the definition of the governance and operational model, technical architecture, and metadata framework, along with the development and internal testing of the first version of the portal. The Implementation and Launch phase (M1–M18) covers the publication of the first set of training offers from consortium partners and their integration into the portal. The Operation and Continuous Improvement phase (M18–M36) encompasses regular updates, performance monitoring, and user feedback collection to enhance functionality and visibility.

With respect to long-term sustainability, several potential continuation pathways exist. The most realistic long-term scenario involves the integration of the CYCERONE portal or its catalogue with the European Cybersecurity Skills Academy initiative [5], which aims to consolidate EU-level cybersecurity training offers. The portal's lightweight design and open metadata structure make such integration technically feasible. Alternatively, the portal could be connected to the Digital Skills and Jobs Platform [21], with the CYCERONE catalogue providing a thematic focus on cybersecurity skills and reskilling programmes. Community-level initiatives such as ECCO [23] offer further federation opportunities. In a minimal scenario, the portal's content could be preserved as a static, publicly accessible archive on the project website.

The governance model is intentionally modular, enabling adjustments to procedures, responsibilities, and workflows without formal restructuring. This adaptability ensures continuity of governance throughout the project and supports the portal's capacity for integration, growth, and continued relevance beyond the project's lifecycle.

6. Conclusions

This deliverable has presented the intermediate version of the CYCERONE portal concept and course format offering. It has established the conceptual and structural foundation on which the cybersecurity training offering of the consortium is built, and it has set the framework within which the specific course catalogue (presented in the companion deliverable D4.5) is populated and will continue to evolve until the end of the project.

Three contributions are central to this deliverable.

First, the terminology framework introduced in Section 2 aligns the CYCERONE vocabulary with the ENISA European Cybersecurity Skills Framework and the EN16234-1 European e-Competence Framework, ensuring that every Course, Training Module, and Resource is described in terms that are interoperable with the broader European cybersecurity education ecosystem. Roles, Skills, Knowledge, and e-Competences provide the common language through which trainees, employers, and partners can interpret and compare the offering.

Second, the organisation of the training offering presented in Section 3 introduces a three-pillar architecture (Awareness, Foundations, Hands-On) supported by a common course schema and a competence-driven Learning Path design. This structure responds directly to the findings of D4.4, which identified the persistent theory–practice divide as the most significant challenge in cybersecurity education, and it provides a clear pedagogical progression from foundational literacy to practical mastery.

Third, the collaborative model described in Section 4 establishes the curatorship, sharing, language, and delivery practices through which 11 universities from 8 different countries can jointly produce, harmonise, and deliver a coherent training offering, while preserving accountability and respecting the diverse contexts of the consortium partners.

The CYCERONE Education Portal, presented in Section 5, complements these contributions by providing the digital entry point through which the offering becomes discoverable to the target audiences. The portal preserves a clear operational boundary — discovery, lead generation, and catalogue publication remain centralised, while course delivery and enrolment fulfilment remain on partner platforms — and it supports the consortium with a tiered, capability-driven integration model that accommodates the different technical readiness levels of the partners. Together, the training offering concept, the course format, and the Education Portal form a single, coherent educational architecture ready to be populated with concrete courses and delivered to trainees from M18 onwards.

This deliverable is intentionally a design and methodology focused document: it describes what CYCERONE plans to offer and how. The final version (D3.1, due at M36) will complement this design with evidence from actual delivery experience. Specifically, D3.1 will incorporate the trainee feedback collected during the multiple delivery waves (M18–M36), the outcomes of the quality assurance process led under T1.2, the documentation of any updates and refinements applied to the format and to the learning paths during operation, and the lessons learned from the harmonisation work across partners. Several areas have been deliberately left open in this intermediate version and are expected to be developed further between D3.6 and D3.1: the detailed design of the Hands-On pillar (CTF and simulation scenarios), the validation of the delivery format choices through real trainee feedback, the refinement of the reference Learning Paths based on enrolment patterns, and the integration with the EITD Skills Passport and personalised learning pathway engine planned for M18.

Looking beyond the project, the educational architecture presented in this deliverable has been designed with long-term sustainability in mind. The alignment with European reference frameworks, the modular architecture of the Education Portal, the open standards on which the integration is built, and the explicit support for federation with broader EU initiatives, such as the European Cybersecurity Skills Academy and other planned repositories, all ensure that CYCERONE can outlive its project funding cycle and continue to contribute to the European cybersecurity skills landscape. The intermediate validation at M16 confirms that the foundations are in place; the next two years of operation will demonstrate how the design performs in practice and will inform the final consolidation in D3.1.

References

[1] ENISA, *European Cybersecurity Skills Framework (ECSF) — Role Profiles*, European Union Agency for Cybersecurity, September 2022. Available: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

[2] ENISA, *European Cybersecurity Skills Framework (ECSF) — User Manual*, European Union Agency for Cybersecurity, September 2022. Available: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

[3] CEN, *EN 16234-1:2019 — e-Competence Framework (e-CF) — A common European Framework for ICT Professionals in all sectors — Part 1: Framework*, European Committee for Standardization, 2019.

[4] **NIST NICE Framework** *National Institute of Standards and Technology, NICE Workforce Framework for Cybersecurity (NIST SP 800-181 Rev. 1), 2020.*

[5] European Commission, *Communication on the European Cybersecurity Skills Academy*, COM(2023) 207 final, Brussels, 18 April 2023.

[6] European Commission, *Digital Europe Programme (DIGITAL) — Work Programme 2023–2024*, Brussels, 2023.

[7] European Commission, *European Year of Skills 2023*, Decision (EU) 2023/936 of the European Parliament and of the Council, Official Journal of the European Union, 2023.

[8] European Parliament and Council, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, Official Journal of the European Union, L 333, 27 December 2022.

[9] European Parliament and Council, *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation, GDPR)*, Official Journal of the European Union, L 119, 4 May 2016.

[10] European Parliament and Council, *Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act, DSA)*, Official Journal of the European Union, L 277, 27 October 2022.

[11] European Parliament and Council, *Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act)*, Official Journal of the European Union, December 2023.

[12] European Parliament and Council, *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, Official Journal of the European Union, 2024.

[13] European Parliament and Council, *Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*, Official Journal of the European Union, 2024.

[14] World Wide Web Consortium (W3C), *Web Content Accessibility Guidelines (WCAG) 2.1*, W3C Recommendation, 5 June 2018.

[15] OpenAPI Initiative, *OpenAPI Specification, Version 3.0*, Linux Foundation. Available: https://www.openapis.org/

[16] IMS Global Learning Consortium, *Learning Tools Interoperability (LTI) Specification*, 1EdTech Consortium.

[17] CYCERONE Consortium, *Grant Agreement No. 101189986 — CYCERONE: CYbersecurity aCadEmy foR educatiOn and experieNcE*, DIGITAL-2023-SKILLS-05-CYBERACADEMY, 2024.

[18] CYCERONE Consortium, *D4.4 — Skills Gap Report (Intermediate Version)*, Lead: Riga Technical University, M16, 2026.

[19] CYCERONE Consortium, *D3.2 — CYCERONE Platform Governance and Operational Model*, Lead: 28Digital, M14, 2026.

[20] CYCERONE Consortium, *D4.5 — CYCERONE List of Courses and Associated Contents (Intermediate Version)*, Lead: Polytechnic University of Milan, M16, 2026 (companion deliverable).

[21] European Commission, *Digital Skills and Jobs Platform*. Available: https://digital-skills-jobs.europa.eu/

[22] *AKADIMOS — A Federated Aggregator for European Skills Academies*, DIGITAL Europe Programme, 2024.

[23] ECCO — *European Cybersecurity Community Project*, 2024. Available: https://www.eccohubs.eu/