Deliverable D4.5

List of Courses and Associated Contents – Intermediate Version

Contractual Date:	**20.04.2026**
Actual Date:	**28.04.2026**
Grant Agreement No.:	**101189986**
Work Package:	**WP4**
Lead Partner:	**Polytechnic University of Milan**
Authors:	Lorenzo Binosi (Polytechnic University of Milan)
Contributors:	28DIGITAL, Talent Garden, Babeș-Bolyai University

Versioning and contribution history

Version	Date	Author/s	Notes
0.1	10/04/2026	Polytechnic University of Milan	
0.2	28/04/2026	Polytechnic University of Milan	

Partner review table

Version	Reviewer (Partner)	Date	Scope of review	Action taken in document
0.1	28DIGITAL	20/04/2026	Review of the draft	Feedback incorporated
0.1	Tampere University	20/04/2026	Review of the draft	Feedback incorporated
0.1	Talent Garden	22/04/2026	Review of the draft	Feedback incorporated
0.1	Babeș-Bolyai University	23/04/2026	Review of the draft	Feedback incorporated

Executive summary

This deliverable, D4.5, presents the intermediate version of the CYCERONE course catalogue at month 16 of the 36-month project cycle. It is the companion to D3.6, which defines the educational architecture and course format of the CYCERONE training offering: while D3.6 documents how the offering is shaped, D4.5 documents what it contains.

The catalogue comprises thirty-six courses organised across three pillars: Awareness, Foundations, and Hands-On. These courses were consolidated from the 48-course baseline defined in the Grant Agreement through a consortium-wide harmonisation process. This process compared the initial baseline with the existing training material, expertise, and educational assets available across the consortium; mapped the resulting inventory against the ENISA European Cybersecurity Skills Framework and the European e-Competence Framework; and assessed its relevance against the skills gaps identified in D4.4.

The **Awareness pillar** comprises eight short courses that provide baseline cybersecurity literacy for every professional in SMEs or in public administrations.

The **Foundations pillar** contains twenty-three courses organised in four tiers:

- Tier 1 (For All Audiences), four advanced awareness courses;
- Tier 2 (Technical Foundations), nine courses addressing the six technical ECSF Roles with an emphasis on laboratory-based content;
- Tier 3 (Management and Governance), six courses for CISO, Risk Manager, Auditor, and Cyber Legal audiences; and
- Tier 4 (Transversal Specialisations), four courses covering specialised topics that complement multiple cybersecurity Roles, including applied cryptography, threat modelling, AI for cybersecurity, and software supply chain security.

The **Hands-On pillar** contains five standalone practical events in which trainees apply the skills acquired in the other pillars to realistic scenarios.

The catalogue provides coverage of all twelve ECSF Roles, while deliberately prioritising those most relevant to the CYCERONE target groups. Roles more likely to be exercised internally by SMEs and public administration bodies receive broader and more structured coverage, while roles more commonly outsourced or associated with specialised providers receive more selective coverage. The deliverable also presents indicative learning paths showing how courses can be combined into structured progressions from baseline awareness to role-oriented competence and, where appropriate, practical application.

As an intermediate deliverable, the catalogue is not final. Between M18 and M36, multiple delivery waves will generate feedback from trainees, instructors, course curators, and partner organisations. This evidence will be used to assess whether courses require minor adjustments, substantial redesign, replacement, or integration with additional material. The final version of the catalogue, to be delivered in D4.2 at M36, will therefore reflect both the methodological consolidation presented in this deliverable and the lessons learned from actual course delivery.

List of contents

List of tables

1. Introduction

Cybersecurity is now one of the most important and rapidly growing professional areas in the European Union. As organisations continue to digitalise their services and operations, they face more frequent and sophisticated cyber threats. At the same time, new and evolving regulatory frameworks, including NIS2 [7], GDPR [8], the Cyber Resilience Act [14], and the AI Act [13], are increasing the need for qualified cybersecurity professionals across the economy. This need is especially strong among Small and Medium-sized Enterprises (SMEs) and public administration bodies, which often do not have sufficient internal expertise or access to structured training opportunities. For this reason, reducing the cybersecurity skills gap has become a strategic priority at the European level, as shown by initiatives such as the European Year of Skills 2023 [6] and the European Cybersecurity Skills Academy [4] launched by the European Commission.

CYCERONE (*CYbersecurity aCadEmy foR educatiOn and experieNcE*) [9] is a European project in cybersecurity education and professional development that aims to contribute to this priority. Funded under the EU Digital Europe Programme [5], the project involves 16 organisations from 10 EU countries, including 11 higher education institutions. During its 36-month duration, CYCERONE develops and delivers a common cybersecurity training offer for professionals in SMEs and public administration. The programme focuses on practical training, role-based learning, and the development of concrete cybersecurity competences.

This deliverable, D4.5, is the intermediate version of the CYCERONE course catalogue. It is released in month 16, together with the companion deliverable D3.6 [12], which defines the educational architecture into which the courses presented here are integrated. D4.5 and D3.6 are the joint intermediate outcomes of Task 3.1 (format design) and Task 4.2 (content harmonisation). The purpose of this deliverable is to list and describe the courses that populate the three-pillar training offering defined in D3.6 at its intermediate stage: it shows how the Awareness, Foundations, and Hands-On pillars are filled with content produced by the consortium partners, how the courses are allocated to partners in a way that avoids duplication and covers the identified gaps, how the courses map to the ECSF Roles and the associated Skills, Knowledge, and e-Competences, and how the catalogue as a whole responds to the skills gap findings documented in D4.4 [10].

1.1 Methodology

The catalogue presented in this deliverable was assembled through a consortium-wide consultation process conducted between the start of the project and month 16. The starting point for this work was the 48-course baseline defined in the Grant Agreement [9], which provided the initial reference for the expected scope of the CYCERONE training offer. This baseline was then compared with the actual cybersecurity-related course offerings, modules, resources, and areas of expertise available across the consortium. Each partner presented its existing training material and expertise to the rest of the consortium, producing a shared course inventory: a consolidated view of both the planned catalogue and the educational assets the consortium collectively held at the start of the project.

Starting from this shared inventory, the consortium conducted a systematic analysis of the existing course materials against two European reference frameworks. The primary reference was the ENISA European Cybersecurity Skills Framework (ECSF) [1, 2], which provides the 12 Role profiles and the associated Skills, Knowledge, and e-Competences against which each course can be mapped. The secondary reference was the European e-Competence Framework [3], which provided the e-Competence vocabulary used to characterise the professional dimensions of each course. For each inventory entry, the responsible partner identified which ECSF Roles the course would address and which Key Skills, Knowledge items, and e-Competences it would develop.

The structured inventory was then compared against the needs of the target audience using the Skills Gap Analysis documented in D4.4 [10]. The analysis highlighted two categories of skills gaps among the target groups. On the

technical side, the target audience reported insufficient practical experience, limited familiarity with the tools and platforms used in professional cybersecurity practice, and a persistent gap between theoretical knowledge and its application in realistic scenarios. On the transversal side, competences such as problem-solving, teamwork, and communication were consistently identified as underdeveloped, despite being essential to the effective practice of cybersecurity in organisational settings.

In response to these findings, and in coordination with the format-design work documented in D3.6 [12], the consortium adopted a three-pillar architecture as the organising principle for the catalogue. This architecture reflects the different levels of need identified across the target audience. The Awareness pillar offers short, accessible courses to develop baseline cybersecurity literacy for any professional who faces cybersecurity-related risks in their daily work, regardless of technical background. The Foundations pillar provides structured, role-oriented training addressing the Skills, Knowledge, and e-Competences required by specific ECSF Roles and by adjacent professional profiles in SMEs and public administration. The Hands-On pillar responds directly to the practical skills gap identified in D4.4, offering scenario-based activities, laboratories, simulations, and exercises in which trainees apply the knowledge acquired in the other pillars to realistic cybersecurity situations.

The combined picture from the framework mapping, the Skills Gap Analysis, and the three-pillar architecture drove the consolidation of the catalogue from the 48-course baseline defined in the Grant Agreement [9] to the 36 courses presented in this intermediate version. The consolidation was treated as a harmonisation and design step aimed at improving the coherence, usability, and pedagogical focus of the CYCERONE offer, rather than as a simple numerical reduction. Existing partner courses were therefore not transferred into the catalogue unchanged. Instead, they were reviewed, adapted, and, where necessary, re-scoped to fit the CYCERONE educational architecture, the three-pillar structure, and the needs of SMEs and public administration professionals.

Courses presenting substantial overlap in objectives and competence coverage were merged or restructured to avoid duplication and create broader, more coherent catalogue entries. Courses that appeared less directly relevant to the target groups, after comparison with the Skills Gap Analysis, were not retained in the intermediate catalogue. Existing material was also improved to strengthen the practical, applied, and competence-oriented dimension of the catalogue, ensuring that both technical and transversal skills gaps identified in D4.4 were addressed across the three-pillar structure. At the same time, the consortium designed learning paths tailored to the identified target groups, organising the catalogue entries into coherent progressions that guide trainees from foundational knowledge to the level of competence required by their target ECSF Role.

Finally, between M18 and M36, multiple delivery waves will provide evidence from actual training implementation, including feedback from trainees, instructors, course curators, and partner organisations. This feedback will be used to assess whether individual courses require minor adjustments, substantial redesign, replacement, or integration with additional material. The final version of the catalogue, to be delivered in D4.2 at M36, will therefore reflect both the methodological consolidation described above and the lessons learned from course delivery.

1.2 Relationship with Other Deliverables

This deliverable is closely connected to several other project outputs:

- **D3.6 (Platform Concept and Course Format Offering — Intermediate Version [12], Polytechnic University of Milan, M16):** The companion deliverable that defines the educational architecture, terminology, and course format used by this catalogue. D3.6 defines the framework; D4.5 populates it.

- **D4.4 (Skills Gap Report — Intermediate Version [10], Riga Technical University, M16):** Provides the foundation for the format design, identifying the most critically valued cybersecurity competencies and preferred learning formats.

- **D3.2 (CYCERONE Platform Governance and Operational Model [11], 28DIGITAL, M14):** Defines how the platform is governed and operated, informing the format design constraints.

- **D4.2 (CYCERONE List of Courses and Associated Contents — Final Version, Polytechnic University of Milan, M36):** The final version of this document incorporates the final list of courses.

- **D3.4 (Digital Platform and User Manual, 28DIGITAL, M36):** The Education Portal implementation.

1.3 Partner Acronyms and Affiliations

The CYCERONE consortium comprises sixteen organisations from ten EU Member States, including eleven higher education institutions. This deliverable refers to partners by their short acronyms throughout; the 12 partners who curate or contribute to courses in D4.5 are listed in the following table.

Acronym	Full Organisation Name	Country
POLIMI	Politecnico di Milano (Polytechnic University of Milan)	Italy
UNITN	Università degli Studi di Trento (University of Trento)	Italy
ELTE	Eötvös Loránd Tudományegyetem (Eötvös Loránd University)	Hungary
UBB	Universitatea Babeș-Bolyai (Babeș-Bolyai University)	Romania
AaltoEE	Aalto University Executive Education	Finland
RTU	Rīgas Tehniskā Universitāte (Riga Technical University)	Latvia
NTUA	Εθνικό Μετσόβιο Πολυτεχνείο (National Technical University of Athens)	Greece
LiU	Linköpings Universitet (Linköping University)	Sweden

RISE	Research Institutes of Sweden	Sweden
TAU	Tampereen Yliopisto (Tampere University)	Finland
KTH	Kungliga Tekniska Högskolan (Royal Institute of Technology)	Sweden
ULUS	Universidade Lusófona (Lusófona University)	Portugal

Table 1: Partner acronyms and affiliations.

1.4 Structure of This Document

The remainder of this document is organised as follows.

Section 2 provides a consolidated overview of the catalogue: its size, the allocation of courses to partners, and the criteria that governed the allocation decisions.

Sections 3 through 7 present the courses themselves, one section per pillar or tier:

- Section 3 covers the Awareness pillar,
- Section 4 covers Tier 1 (Foundations pillar),
- Section 5 covers Tier 2 (Foundations pillar),
- Section 6 covers Tier 3 (Foundations pillar),
- Section 7 covers Tier 4 (Foundations pillar),
- Section 8 covers the Hands-On pillar.

Section 9 analyses the coverage of the catalogue against the twelve ECSF Role profiles and presents the learning paths designed for the identified target groups.

Section 10 presents the conclusions.

2. Catalogue Overview

This section provides a consolidated view of the CYCERONE course catalogue at its intermediate stage. It presents the total number of courses in each pillar and tier, the allocation of courses to the consortium partners, and the criteria that governed the allocation decisions.

2.1 Catalogue Size and Distribution

The intermediate CYCERONE catalogue comprises thirty-six courses across three pillars: Awareness, Foundations, and Hands-On. The distribution is summarised in the following table.

Pillar / Tier	Courses	Short description
Awareness	8	Short, accessible courses providing baseline cybersecurity literacy for every learner.
Foundations — Tier 1	4	Advanced awareness for all audiences, longer and more structured than Awareness.
Foundations — Tier 2	9	Technical Foundations for the six technical ECSF Roles.
Foundations — Tier 3	6	Governance, risk and compliance for CISO, Risk Manager, Auditor, and Cyber Legal audiences.
Foundations — Tier 4	4	Specialised topics that complement multiple cybersecurity Roles.
Hands-On	5	Standalone practical events: CTFs, labs, and simulations.

Table 2: CYCERONE course catalogue size and distribution by pillar and tier.

2.2 Courses Allocation

Each partner contributes as a curator for a limited number of courses in the catalogue. The allocation methodology is defined in Section 2.3, while the course distribution is summarised in the following table. Finally, the Hands-On courses will be co-curated by all the partners.

Partner	Awareness	Tier 1	Tier 2	Tier 3	Tier 4	Total
POLIMI	Digital Forensics	—	Reverse Engineering &	—	Applied Cryptography,	4

	Fundamentals		Binary Analysis		Threat Modelling	
UNITN	—	—	Web Security, Cloud Security	—	—	2
ELTE	Social Engineering	Social Engineering	—	—	Software Supply Chain Security	3
UBB	Cybersecurity Awareness	Applied Cybersecurity	Network and IoT Security	—	—	3
AaltoEE	Security Compliance	—	—	Business Continuity and Digital Resilience	—	2
RTU	—	—	Digital Forensics, Cybersecurity Architecture	Cybersecurity Management Fundamentals	—	3
NTUA	AI and Cybersecurity	—	Security Orchestration and Automation	—	—	2
LiU	Risk Management Fundamentals	—	—	Risk Management for Organisations	—	2
RISE	—	—	—	Cybersecurity for Management, Cybersecurity for Journalists	—	2
TAU	Fault Tolerance in Automation	Cybersecurity for Everyone	Secure Software Development	—	—	3
KTH	—	—	Software Safety and Security	Information Security Management for Public Administration	—	2

ULUS	Privacy	Privacy Foundations	—	—	AI for Cybersecurity	3

Table 3: Course allocation by partner and catalogue pillar/tier.

2.3 Allocation Decisions

The allocation of courses to partners was the result of a structured analysis carried out in consultation with the consortium partners. Three factors, applied in the following order of priority, drove every allocation decision.

1. **Existing partner courses.** The consortium partners collectively submitted an extensive inventory of courses that they already offer, often as part of their ordinary teaching activities. The CYCERONE catalogue was built on top of this existing offering: partners were not asked to develop new courses from scratch. Instead, as reported in the methodology (Section 1), partners were asked to refactor and improve the modules and the resources of their courses based on the results of the Skills Gap Analysis. Whenever an inventory entry corresponded to a topic needed by the catalogue, that entry became the source material for the corresponding catalogue course, possibly after scoping and translation.

2. **Partner expertise.** Courses were assigned to partners based on their area of expertise. Some partners are more suited to management and governance courses, whereas others have a stronger track record in technical content.

3. **Partner budget.** Partners were assigned several courses that reflect the training-related effort allocated to them in the Grant Agreement. Partners with a larger budget are expected to contribute a proportionally larger share of the catalogue, whereas partners with a smaller budget contribute fewer or smaller courses. This criterion acts as a tiebreaker and an overall fairness check: when two partners could reasonably curate the same course, the one with the larger training budget was preferred.

2.4 Managed Overlaps Across the Catalogue

The consolidation process described in Section 1.1 removed or reduced unnecessary duplication across the catalogue. However, some degree of overlap between courses remains intentional and pedagogically justified. Because cybersecurity competences are cumulative and context-dependent, the same broad topic may appear at different levels of depth, for different target audiences, or in different application contexts.

First, several topics appear both in the Awareness pillar and in the Foundations pillar. In these cases, the overlap reflects the progression defined in the three-pillar architecture rather than duplication. Awareness courses introduce baseline concepts for professionals who need cybersecurity literacy in their daily work, regardless of technical background. Foundations courses address the same or related domains at a greater level of depth, with stronger alignment to ECSF Roles, Skills, Knowledge, and e-Competences.

Second, some organisational topics, such as risk management, governance, compliance, continuity, and incident management, appear across multiple courses because they correspond to different responsibilities within SMEs and public administration bodies. A manager, a risk owner, a compliance officer, and a technical incident responder may all need to understand related concepts, but from different operational, legal, strategic, or technical perspectives.

Third, several technical courses share common security concepts, tools, or methods, such as vulnerability analysis, secure configuration, threat modelling, or secure development. These overlaps are retained where the shared competence is applied in a distinct technical context, for example web applications, cloud environments,

networks, software systems, or supply chains. In such cases, the overlap supports transferability of competences across domains while preserving the specific learning outcomes of each course.

Finally, the Hands-On pillar deliberately builds on knowledge and skills developed in the Awareness and Foundations pillars. Any overlap between hands-on activities and previous courses is therefore functional: the purpose of these activities is not to introduce a separate body of content, but to allow trainees to apply previously acquired competences in realistic, scenario-based settings.

3. Awareness Pillar

The Awareness pillar comprises eight short courses that provide baseline cybersecurity literacy for all employees in SMEs or public administration. The courses are self-contained and can be taken independently of each other; they are designed to be accessible to non-technical professionals and suitable for delivery as self-paced, asynchronous online courses. Finally, courses in this pillar range from 6 hours (1 day) to 30 hours (1 week).

The following subsections describe each course in the Awareness pillar. For each course, the subsection records the course title, the Curator partner, the level (beginner, intermediate, advanced, or mixed), a short description and the learning outcomes of the course.

3.1 Privacy

Curator: ULUS · **Level:** Beginner

Short description: This course provides trainees with the essential knowledge and skills to navigate the modern data landscape safely and responsibly. It bridges the gap between legal rights and practical online behaviour, empowering participants to become privacy-competent users of technology. Participants will explore the fundamental rights of data subjects under personal data protection regulations and learn how to exercise these rights in real-world scenarios. The course also covers how to identify information privacy breaches, analyse past incidents, evaluate privacy policies, recognise social engineering techniques, and use privacy-enhancing technologies to safeguard sensitive information. Designed for employees, students, and general internet users, this course is ideal for anyone who uses digital applications or handles personal information in personal or professional contexts.

Learning outcomes:

- Identify at least three common social engineering techniques (e.g., phishing, pretexting, baiting) used to compromise personal data in real-world scenarios.
- Analyse a given privacy policy to determine whether it contains essential elements (e.g., data collection scope, retention period, user rights) and flag missing or misleading provisions.
- Evaluate past information privacy breaches to explain the impact on affected data subjects, including financial, reputational, or psychological harm.
- Implement at least two privacy-enhancing technologies (e.g., a browser extension or software tool) to secure personal data during routine internet use.
- Distinguish between a privacy-aware user and a privacy-competent user by describing specific behaviours and competencies each would demonstrate when using an IT application.

- Demonstrate the correct procedure for exercising a data subject's right (e.g., right to access or right to erasure) by drafting a valid request to a data controller.

Target ECSF Roles: Cybersecurity Educator (primary); all ECSF roles (secondary — privacy awareness and data-protection principles are relevant to every cybersecurity professional).

3.2 Social Engineering

Curator: ELTE · **Level:** Beginner

Short description: This course provides a brief introduction to the key aspects of social engineering, highlighting the psychological triggers, major types of attacks, and possible mitigation techniques. The importance and the main basic and advanced psychological triggers are introduced first. The most important attack methods are summarised through examples and use cases, including phishing and its variants, whaling, baiting, and physical security. Special focus on AI-based attacks, including Deepfakes and LLM-based methods. The legal background is also introduced at a basic level, and various detection and defence strategies are suggested, especially for the corporate environment.

Learning outcomes:

- Identify social engineering attack surfaces.
- Identify social engineering countermeasures.
- Evaluate the security culture of the employees.
- Develop security awareness training materials.
- Implement security awareness training.

Target ECSF Roles: Cybersecurity Educator (primary); all ECSF roles (secondary — social engineering recognition is a baseline competence for every cybersecurity professional).

3.3 Cybersecurity Awareness

Curator: UBB · **Level:** Beginner

Short description: This is an introductory course designed to equip participants with essential knowledge and practical skills to safely navigate today's digital environment. It covers fundamental concepts such as the importance of cybersecurity, common threats including phishing and malware and the role of human factors in security incidents. The course emphasises safe online behaviour, strong authentication practices and basic system hygiene, while introducing key protective tools such as antivirus software, firewalls and VPNs. Participants will also learn how to recognise and respond to potential security risks, protect personal and organisational data and apply secure practices when using workplace applications. By the end of the course, learners will develop a security-conscious mindset and the ability to minimise everyday cybersecurity risks in both personal and professional contexts.

Learning outcomes:

- Understand key cybersecurity concepts and threats.

- Identify and avoid social engineering attacks.
- Apply best practices for secure digital behaviour.
- Use basic security tools (AV, firewall, VPN, backups).
- Demonstrate responsible and security-aware behaviour.

Target ECSF Roles: Cybersecurity Educator (primary); all ECSF roles (secondary — baseline cybersecurity hygiene applies to every professional regardless of Role).

3.4 Security Compliance

Curator: AaltoEE · **Level:** Beginner

Short description: This course provides a foundational understanding of information security and cybersecurity in an increasingly digitalised operating environment, focusing on common risks, technologies, and sector-specific challenges. It supports learners in developing awareness of how security risks emerge, materialise, and are shaped by digitalisation, regulation, and industry context, enabling more informed and responsible decision-making in their professional roles. This course is designed for non-technical professionals who need a practical, foundational understanding of information security and cybersecurity from a compliance and risk perspective, particularly in roles involving data handling, oversight responsibilities, or organisational decision-making.

Learning outcomes:

- Explain the core concepts and objectives of information security and cybersecurity, and their role in protecting organisational data, systems, and operations.
- Identify common information security and cybersecurity risks and describe how these risks materialise into incidents in real-world organisational contexts.
- Explain how digitalisation and emerging technologies—such as artificial intelligence, cloud services, and distributed ledger technologies—affect security risks and organisational exposure.
- Compare cybersecurity challenges across industries, recognising how sector-specific regulations, operating environments, and threat landscapes influence security priorities.

Target ECSF Roles: Cyber Legal, Policy and Compliance Officer (primary); CISO, Cybersecurity Risk Manager (secondary — compliance awareness is essential for anyone involved in governance or risk decisions).

3.5 AI and Cybersecurity

Curator: NTUA · **Level:** Beginner

Short description: This course introduces the basic concepts at the intersection of Artificial Intelligence (AI) and Cybersecurity, with a focus on everyday applications and risks. It is designed for a broad audience with no technical background and aims to raise awareness of how AI is increasingly used in digital environments. Participants will learn how AI supports cybersecurity activities such as detecting suspicious behaviour, identifying threats, and assisting in automated responses. The course also highlights how attackers can exploit AI technologies, including examples such as deepfakes, AI-generated scams, and phishing attacks. In addition, the course covers key principles for the safe and responsible use of AI, including data protection, confidentiality, and

awareness of potential misuse. By the end of the course, participants will be able to recognise common AI-related cybersecurity risks and understand how AI impacts both security and everyday digital practices.

Learning outcomes:

- Identify basic concepts of Artificial Intelligence and its role in cybersecurity.
- Recognise how AI is used to support cybersecurity operations.
- Identify common cyber threats that use AI (e.g. deepfakes, phishing scams).
- Describe risks related to the unsafe use of AI tools.
- Apply basic principles for safe and responsible use of AI.
- Recognise key challenges in securing AI systems (e.g. privacy, robustness).

Target ECSF Roles: Cybersecurity Educator (primary); all ECSF roles (secondary — awareness of AI-enabled threats, AI-based defence tools, and AI Act obligations is relevant to every cybersecurity professional).

3.6 Risk Management Fundamentals

Curator: LiU · **Level:** Beginner

Short description: This introductory course covers the basic theory and practice of cybersecurity risk management in organisations. The course material includes an introduction to general risk management and identification, progressing to relevant standards, and tools for threat modelling and risk assessment. Learners will engage in practical tasks to complement the theory learned during the course.

Learning outcomes:

- Gain familiarity with risk management standards.
- Identify common cybersecurity risks.
- Use basic risk management tools and frameworks.
- Evaluate and mitigate identified risks.
- Apply theory to a practical risk management example.

Target ECSF Roles: Cybersecurity Risk Manager (primary); CISO (secondary — risk identification and basic risk management frameworks are foundational to both Roles at the awareness level)

3.7 Digital Forensics Fundamentals

Curator: POLIMI · **Level:** Beginner

Short description: This course prepares participants to make sound decisions when digital forensics enters their professional lives. Organisations may one day face an incident, such as a ransomware attack, a suspected insider, a compromised email account, or a lost device containing personal data, where the first hours of decisions

determine whether evidence is preserved or destroyed, whether an investigation succeeds or collapses, and whether the organisation meets its obligations or compounds its problems. The course is deliberately non-technical. Rather than training participants to perform forensic analysis themselves, it equips them to recognise when forensics are needed, to avoid common mistakes that irreversibly damage evidence, to commission and oversee external forensic services competently, and to put baseline readiness measures in place before an incident occurs. Real-world case studies anchor the learning in situations participants are realistically likely to encounter. Content spans the nature of digital evidence and the investigation lifecycle; practical first-response actions for non-specialists; the specific realities of forensics in cloud and SaaS environments, where most organisational data now lives; the contemporary threat landscape; and a closing module on building minimal but effective readiness.

Learning outcomes:

- Explain what digital forensics is, how it relates to incident response, and what kinds of digital evidence exist in a typical organisational environment.
- Describe the stages of a forensic investigation from the perspective of the organisation commissioning the work.
- Recognise the early signals of a security incident and take appropriate first-response actions, avoiding common mistakes that destroy evidence.
- Identify the distinctive characteristics and limitations of forensics across computer, mobile, network, email, and cloud or SaaS environments.
- Recognise the typical modus operandi of common threats, including ransomware, business email compromise, invoice fraud, insider data theft, and account takeover.
- Commission external forensic services competently, including how to evaluate a provider and what to expect from a forensic report.
- Implement baseline readiness measures appropriate to a resource-constrained organisation.
- Know where to find authoritative resources for further guidance.

Target ECSF Roles: Digital Forensics Investigator (primary); Cyber Incident Responder (secondary — awareness of the cybercrime landscape and the forensics investigation lifecycle support incident recognition and evidence preservation).

3.8 Fault Tolerance in Automation

Curator: TAU · **Level:** Mixed

Short description: This course provides an introductory overview of cybersecurity, risk awareness, fault tolerance, and safety in industrial automation environments. It is designed for professionals who work with or around automated and cyber-physical systems but are not cybersecurity specialists. By the end of the course, trainees will understand why cybersecurity and fault tolerance are critical for industrial systems, recognise common threats and faults, appreciate the role of standards and regulations, and know how human factors and operational practices influence safety and resilience.

Learning outcomes:

- Why cybersecurity is critical in automation environments; impact of breaches on safety, productivity, and reputation.
- What SCADA and ICS systems are, and how they are vulnerable to cyber threats.
- Security principles and their relevance in automation.
- Overview of IEC 62443, NIST CSF, and ISO 27001 relevant to automation.
- How to identify and assess risks in automation systems common faults.
- Common faults in operational technology.
- Common security mechanisms in operational technology.
- How and why to report and handle faults and cybersecurity incidents.

Target ECSF Roles: Cybersecurity Implementer (primary); Cybersecurity Architect (secondary — awareness of OT threats, industrial automation resilience, and fault-tolerance principles supports both the implementation and the architectural design of resilient automation systems).

4. Foundations Pillar – Tier 1

Tier 1 of the Foundations pillar comprises four courses that extend the Awareness content into a more structured and substantial offering, still accessible to every professional in an SME or public administration, regardless of their specific role. Tier 1 courses do not presume any technical cybersecurity background from the trainee; they are designed as an advanced awareness layer for professionals who want to deepen their understanding of cybersecurity without pursuing a technical or management specialisation. The courses are self-contained and can be taken independently of each other; they are suitable for delivery as self-paced, asynchronous online courses or in a blended format. Courses in this tier span 20 to 60 contact hours.

The following subsections describe each course in Tier 1. For each course, the subsection records the course title, the Curator partner, the level (beginner, intermediate, advanced, or mixed), a short description and the course learning outcomes.

4.1 Cybersecurity for Everyone

Curator: TAU · **Level:** Beginner

Short description: This course provides a broad introduction to cybersecurity from the perspectives of society, organisations, and individuals. It aims to increase cybersecurity awareness and support the adoption of secure practices in everyday digital activities. Participants will learn how cybersecurity affects daily life, professional environments, business operations, and wider society, while developing a practical understanding of common risks and protective behaviours. The course is designed for all learners, regardless of educational background or profession. Beginners will acquire a solid foundation in cybersecurity concepts, while more experienced participants may gain new perspectives on the social, organisational, and individual dimensions of cybersecurity.

Learning outcomes:

- Explain what cybersecurity means and why it is important for individuals, organisations, and society.
- Recognise that cybersecurity is a shared responsibility involving users, organisations, service providers, and public institutions.
- Identify how individual behaviour can influence cybersecurity in everyday digital activities.
- Apply basic password security practices, including the use of strong passwords, password managers, and multi-factor authentication.
- Detect common characteristics of phishing messages and other social engineering attempts.
- Recognise basic information influence activities, including misleading content, manipulation attempts, and coordinated disinformation.
- Apply simple preventive measures to reduce exposure to cyber threats and information manipulation.

Target ECSF Roles: Cybersecurity Educator (primary); all ECSF roles (secondary — baseline cybersecurity awareness, secure behaviour, phishing recognition, password hygiene, and understanding of shared cybersecurity responsibility are relevant to every cybersecurity professional).

4.2 Privacy Foundations

Curator: ULUS · **Level:** Mixed

Short description: This course introduces trainees to the concept of privacy and its foundations in relation to personal and sensitive data exchanged across different environments. It provides a structured understanding of privacy terminology, Personally Identifiable Information (PII), safeguarding requirements, legal considerations, and privacy controls based on ISO 29100 and ISO 29151. Participants will explore the implementation of a Privacy Information Management System (PIMS), including how ISO 27001, ISO 27002, and ISO 27701:2025 can be integrated into privacy governance and management practices. The course also covers privacy engineering, showing how privacy can be embedded into system and security engineering throughout the full system lifecycle. Trainees will learn how to apply privacy-by-design principles to products and services, including user interface design and PII end-of-life procedures. The course also introduces privacy requirements engineering methodologies, such as goal-oriented, risk-oriented, and threat-driven approaches, including the LINDDUN framework. It is designed for privacy officers, information security managers, system architects, software engineers, compliance professionals, and IT project managers.

Learning outcomes:

- Classify a given set of data elements as Personally Identifiable Information (PII) or special categories of data according to the ISO 29100 structural framework.
- Map at least five ISO 29100 privacy principles to corresponding privacy controls from a provided control list.
- Implement a Privacy Information Management System (PIMS) by documenting how ISO 27001:2022 requirements will be integrated into an existing organizational structure per ISO 27701:2025.
- Integrate privacy engineering practices into a given system lifecycle phase (e.g., requirements, design, testing, or decommissioning) by specifying at least three privacy-related activities for that phase.

- Design a privacy-by-design prototype for a product or service that includes: a human-computer interface element addressing privacy, a communication requirement, and an end-of-life procedure for PII.

- Apply the LINDDUN threat-driven methodology to a given system description to identify at least four distinct privacy threats and propose corresponding mitigations.

Target ECSF Roles: Chief Information Security Officer (CISO), Cybersecurity Architect, Cyber Legal, Policy and Compliance Officer (primary); Cybersecurity Risk Manager, Cybersecurity Implementer (secondary).

4.3 Social Engineering

Curator: ELTE · **Level:** Mixed

Short description: The course aims to provide a deeper understanding of the main psychological and technical background of social engineering by offering a more detailed overview of the latest offensive and defensive tools and techniques. The detailed theoretical background is followed by practical examples and simple exercises. Both the psychological and technical backgrounds are considered. On the offensive side, the core social engineering attack methods are described, including phishing, vishing, whaling, baiting, and physical security. The course covers advanced social engineering attacks using AI, especially GenAI- and LLM-based techniques, as well as impersonation attacks such as voice cloning and Deepfakes. On the defensive side, the legal aspects and the detection mechanisms are described.

Learning outcomes:

- Identify social engineering attack surfaces.
- Identify social engineering countermeasures.
- Evaluate the employees' security culture.
- Develop security awareness training materials.
- Implement security awareness training.

Target ECSF Roles: Cybersecurity Educator (primary); all ECSF roles (secondary — social engineering recognition is a baseline competence for every cybersecurity professional).

4.4 Applied Cybersecurity

Curator: UBB · **Level:** Mixed

Short description: The Applied Cybersecurity course is, as its name implies, a practical course designed to build on foundational cybersecurity knowledge and equip participants with real-world skills to recognise, analyse and respond to common cyber threats. Through interactive exercises, simulations and case studies, learners will gain experience in identifying phishing emails, malicious links and social engineering attacks, as well as applying safe digital practices across devices, office applications and online platforms. The course also provides hands-on exposure to essential security tools such as antivirus software, firewalls, VPNs, password managers and Multi-Factor Authentication (MFA). By completing this course, participants will develop a proactive, security-conscious mindset, the ability to implement protective measures in practical scenarios and the competence to contribute to a culture of cybersecurity awareness in personal and organisational contexts.

Learning outcomes:

- Apply cybersecurity knowledge in real-world scenarios.
- Identify, analyse, and respond to cyber threats.
- Use security tools and safe practices effectively.
- Develop proactive and responsible cybersecurity behaviour.
- Promote cybersecurity awareness and best practices within personal and organisational contexts.

Target ECSF Roles: All profiles (foundational); particularly Cyber Incident Responder and Cybersecurity Implementer.

5. Foundations Pillar – Tier 2

Tier 2 of the Foundations pillar is the technical core of the CYCERONE catalogue. It comprises nine courses that together address the most technical roles. Tier 2 courses are laboratory-oriented in response to the Skills Gap Analysis finding that the lack of hands-on experience is the most significant shortcoming in cybersecurity education. Trainees are expected to have a cybersecurity background consistent with the prerequisites of each specific course. The courses are self-contained and can be taken independently of each other. However, some natural progressions exist (for example, from a beginner to an advanced course on the same topic). Due to the laboratory component, most Tier 2 courses are delivered synchronously or in a blended format rather than fully asynchronously. Courses in this tier have a duration that varies from 20 to 100 contact hours.

The following subsections describe each course in Tier 2. For each course, the subsection records the course title, the Curator partner, the level (beginner, intermediate, advanced, or mixed), a short description, and the course's learning outcomes.

5.1 Web Security

Curator: UNITN · **Level:** Advanced

Short description: This course provides a structured introduction to web application security through a combination of concise theory and hands-on exercises. It is designed for learners with basic familiarity with web technologies and general cybersecurity concepts who want to develop practical skills in identifying and exploiting common web vulnerabilities. The course covers how web applications work at a fundamental level, including the HTTP protocol, and examines both server-side and client-side security issues. Topics include input validation flaws, file handling vulnerabilities, injection attacks, authentication and logic weaknesses, and browser-based attacks. Practical learning is delivered through a series of progressively challenging exercises that simulate real-world scenarios, requiring participants to analyse application behaviour, identify weaknesses, and apply appropriate exploitation techniques. After completing the course, participants will be able to systematically assess web applications for common security flaws, understand how these vulnerabilities can be exploited, and interpret the impact of successful attacks.

Learning outcomes:

- Analyse HTTP requests and responses to understand web application behaviour.

- Identify and exploit common server-side vulnerabilities, including file disclosure, path traversal, and injection flaws.
- Apply SQL injection techniques to extract and manipulate data in controlled environments.
- Detect and exploit client-side vulnerabilities such as XSS and CSRF.
- Evaluate application logic to identify authentication and business logic weaknesses.
- Use systematic approaches to enumerate, test, and validate web application attack surfaces.

Target ECSF Roles: Penetration Tester, Cybersecurity Implementer (primary).

5.2 Cloud Security

Curator: UNITN · **Level:** Intermediate

Short description: This course introduces the fundamental principles of cloud security through a combination of targeted theory and hands-on exercises. It is intended for learners with a basic understanding of cloud computing and cybersecurity who want to develop practical skills in identifying and exploiting common security weaknesses in cloud environments. The course focuses on how cloud infrastructures are configured and managed, with particular attention to identity and access management, resource exposure, and common misconfiguration patterns. Participants will work through practical scenarios that simulate real-world cloud deployments, where they must analyse configurations, identify security gaps, and exploit weaknesses in a controlled setting. Topics include insecure access controls, exposed storage resources, credential leakage, and privilege escalation techniques. After completing the course, participants will be able to assess cloud environments for common misconfigurations, understand how attackers move within cloud infrastructures, and evaluate the impact of compromised resources.

Learning outcomes:

- Analyse cloud configurations to identify common security misconfigurations.
- Enumerate cloud resources and assess their exposure and access controls.
- Identify and exploit credential leakage and insecure identity management practices.
- Privilege escalation through misconfigured roles and permissions.
- Assess storage and compute resources for improper access restrictions.
- Apply systematic approaches to analysing and attacking cloud environments.

Target ECSF Roles: Penetration Tester, Cybersecurity Implementer (primary).

5.3 Reverse Engineering and Binary Analysis

Curator: POLIMI · **Level:** Advanced

Short description: This course explores the foundations and advanced concepts of software security with a strong focus on reverse engineering. It covers theoretical and practical topics related to assembly (x86_64/ARM), reverse

engineering (through static and dynamic analysis), and symbolic execution. These topics will help learners inspect binaries, reconstruct their logic, and understand their behaviour — skills that are essential for tasks such as malware analysis and digital forensics. The course also introduces learners to technical tools such as Ghidra/IDA Pro, GDB, and angr, to tackle practical in-class and at-home challenges.

Learning outcomes:

- Read and understand x86_64 and ARM assembly code.
- Analyse compiled binaries using both static and dynamic analysis techniques.
- Use industry-standard tools such as Ghidra, IDA Pro, and GDB to inspect and debug programs.
- Apply symbolic execution with angr to reason about program behaviour and explore execution paths.
- Reconstruct the logic of unknown or obfuscated binaries.
- Identify and analyse malicious software, recognising common malware patterns and techniques.
- Approach practical reverse engineering challenges methodically and independently.

Target ECSF Roles: Digital Forensics Investigator, Cyber Threat Intelligence Specialist, Cybersecurity Researcher (primary); Penetration Tester, Cyber Incident Responder (secondary).

5.4 Network and IoT Security

Curator: UBB · **Level:** Mixed

Short description: Network and IoT Security is a practice-oriented course that introduces fundamental cybersecurity concepts through real-world network configuration and experimentation. The course uses OpenWrt as a flexible, open-source platform to explore how security mechanisms are implemented and managed at the network edge. Participants will gain hands-on experience in configuring and securing network infrastructures, including firewall management, virtual private networks (VPNs), traffic monitoring and routing. The course also addresses security challenges specific to IoT and embedded systems, emphasising practical techniques for system hardening, access control and threat mitigation. Through guided labs and realistic scenarios, learners will develop the ability to design, implement, and troubleshoot secure network environments. The course bridges theoretical cybersecurity foundations with applied skills, preparing participants for roles in network administration, cybersecurity operations and secure system deployment.

Learning outcomes:

- Explain core cybersecurity concepts (CIA triad, common network and IoT threats).
- Design and configure secure network architectures at the edge.
- Implement and manage firewall rules, NAT, and routing.
- Deploy and configure VPNs for secure communication.
- Apply security best practices to IoT and embedded devices.
- Monitor and analyse network traffic using built-in tools.

- Troubleshoot network and security issues effectively.
- Apply ethical practices and communicate security findings clearly.

Target ECSF Roles: Cybersecurity Implementer (primary); Penetration Tester, Cyber Incident Responder (secondary).

5.5 Digital Forensics

Curator: RTU · **Level:** Intermediate

Short description: This course provides a comprehensive understanding of digital investigation processes and their application in modern cyber incident management. It covers the main aspects of digital investigation—from evidence collection and analysis to incident documentation and implementation of solutions—while simulating realistic situations to analyse incident investigation processes from start to finish.

Learning outcomes:

- Develop an understanding of the role of digital investigation and its application in incident recording.
- Develop skills in collecting and using digital evidence from legal and technical aspects.
- Identify, collect, and analyse network and host evidence using appropriate tools and methodologies.
- Structure incident reports and justify recommendations for further security measures.
- Proactively analyse and detect potential threats using digital investigation and incident management methods.
- Identify, recover, document, and analyse digital evidence.

Target ECSF Roles: Digital Forensics Investigator (primary); Cyber Incident Responder, Cyber Threat Intelligence Specialist (secondary);

5.6 Cybersecurity Architecture

Curator: RTU · **Level:** Intermediate

Short description: This course provides theoretical and practical insights into the cybersecurity architecture development process, helping organisations standardise security measures, optimise IT resource management, and ensure business continuity. It covers industry-leading solutions, from integrating DevSecOps principles into software development to using artificial intelligence in cyber threat analysis, preparing students to design and manage secure IT systems.

Learning outcomes:

- Develop an understanding of how cybersecurity architecture is applied to ensure the long-term resilience of the organisation's IT systems and protect against threats.
- Develop the ability to predict technological developments and threats to adapt the organisation's security architecture.

- Implement and apply modern security tools, such as IDS/IPS, VPN, firewalls, log file management, and encryption technologies.
- Prepare architectural documentation and specifications, and develop architectures based on "security and privacy by design".

Target ECSF Roles: Cybersecurity Architect (primary); Cybersecurity Implementer (secondary);

5.7 Security Orchestration and Automation

Curator: NTUA · **Level:** Mixed

Short description: This course introduces the fundamental concepts of cybersecurity orchestration and automation, focusing on how security operations can be enhanced through the integration of tools and automated workflows. It is designed for technical professionals involved in security operations, incident response, or system administration who seek to understand how modern Security Operations Centres (SOCs) improve efficiency and scalability. Participants will learn how cybersecurity tools are connected through orchestration platforms, how playbooks are used to standardise response actions, and how automation can reduce response time and human effort. The course also provides practical examples of workflows and real-world scenarios to illustrate how orchestration supports incident detection, analysis, and response. By the end of the course, participants will be able to understand the role of orchestration in SOC environments, recognise the value of automation in cybersecurity operations, and identify opportunities to improve processes through integration and automated workflows.

Learning outcomes:

- Identify the key components and workflows of Security Operations Centre (SOC) environments
- Explain how cybersecurity orchestration platforms integrate multiple security tools
- Refer to structures and data models
- Analyse incident response processes to identify opportunities for automation
- Describe the structure and purpose of playbooks in automated cybersecurity operations
- Apply basic orchestration concepts to model simple security workflows
- Evaluate the benefits and limitations of automation in cybersecurity operations
- Recognise the importance of tool integration, APIs and interoperability in enabling effective orchestration

Target ECSF Roles: Cyber Incident Responder (primary); Cybersecurity Implementer (secondary).

5.8 Software Safety and Security

Curator: KTH · **Level:** Advanced

Short description: This course introduces fundamental techniques for the rigorous analysis of software systems, with a focus on safety and security properties. Drawing on types, logics, and formal specification, it equips participants with the methods needed to detect undesired or unsafe behaviour in software or to formally

establish its absence. The course combines theoretical foundations with hands-on experience using established tools, allowing learners to apply each technique to concrete software systems. Topics include temporal logics, model checking and formal specification with NuSMV; system modelling and refinement with Event-B and the Rodin platform; verification of concurrent and networked programs with Java Pathfinder; and memory safety analysis and fuzzing using dedicated checkers and fuzzers. Through these techniques, participants will learn to construct models of systems, express safety and security properties precisely, and evaluate the strengths and limitations of different verification and validation approaches. The course is designed for learners who want to go beyond pragmatic secure development practices and engage with the rigorous methods used in safety-critical software and high-assurance system design. By the end of the course, participants will be able to apply formal techniques in professional contexts, adapt verification tools to new problems, and engage critically with discussions on software safety and security from both an expert and a citizen perspective.

Learning outcomes:

- Explain safety and security aspects of software systems and articulate their relevance in professional and societal contexts.
- Construct formal models of software systems suitable for analysis.
- Specify and analyse safety and security properties using temporal logics and formal specification languages.
- Apply analytical tools (NuSMV, Rodin, Java Pathfinder, memory checkers, fuzzers) to verify properties of software systems.
- Evaluate and compare different approaches to the verification and validation of software systems.
- Adapt verification tools and techniques to new problems in professional practice.

Target ECSF Roles: Penetration Tester, Cybersecurity Researcher (primary); Cybersecurity Implementer (secondary).

5.9 Secure Software Development

Curator: TAU · **Level:** Advanced

Short description: This course introduces secure programming principles and practices with the aim of preventing software vulnerabilities as early as possible in the development lifecycle. It focuses on how secure coding, automated security checks, and DevSecOps practices can support better software development and decision-making. Trainees will learn how to build and use a DevSecOps pipeline, interpret the outputs of security tools, apply OWASP guidance, and understand the role of automation in identifying weaknesses before deployment. The course also introduces Software Bill of Materials (SBOM) files, showing how they can be created and used to improve transparency, dependency management, and software supply chain security.

Learning outcomes:

- Identify key security considerations to take into account when implementing software systems.
- Apply secure programming practices to reduce common software vulnerabilities during development.
- Use cryptographic mechanisms appropriately in software development, avoiding common implementation mistakes.

- Implement a basic DevSecOps pipeline integrating automated security checks into the development workflow.
- Use static analysis tools to identify potential security weaknesses in source code.
- Create and use Software Bill of Materials (SBOM) files to improve dependency visibility and support software supply chain security.
- Explain the legal and regulatory requirements relevant to secure software development, with particular attention to GDPR and the Cyber Resilience Act.

Target ECSF Roles: Cybersecurity Implementer (primary); Cybersecurity Architect, Penetration Tester (secondary).

6. Foundations Pillar – Tier 3

Tier 3 of the Foundations pillar comprises six courses that address management, governance, risk, compliance, and sector-specific organisational needs. Tier 3 courses are conceptual and strategic in their content: they do not require a technical cybersecurity background. They are designed for professionals in management or compliance roles who already have working experience in their organisation. The courses are self-contained and can be taken independently of each other; they are typically delivered as self-paced, asynchronous or blended courses, so that trainees can combine them with their daily responsibilities. Courses in this tier have durations ranging from 10 hours to 80 hours.

The following sections describe each course in Tier 3. For each course, the subsection records the course title, the Curator partner, the level (beginner, intermediate, advanced, or mixed), a short description, and the course's learning outcomes.

6.1 Cybersecurity for Management

Curator: RISE · **Level:** Mixed

Short description: This course is for decision-makers and managers seeking to understand cybersecurity from a strategic and business perspective. It focuses on risk management, governance and compliance. It provides practical insights into how organisations can prevent, detect and respond to cyber threats. Participants will gain an overview of the current threat landscape, learn how to align cybersecurity with business objectives and understand their role in supporting resilient and secure operations. The course also covers the use of AI in cybersecurity and its implications for organisational risks.

Learning outcomes:

- Understand key cybersecurity risks and their impact on business operations.
- Identify threats and support risk mitigation, governance and compliance (GDPR, NIS2).
- Make informed decisions, support incident response, and promote security awareness.

Target ECSF Roles: Chief Information Security Officer (CISO) (primary); Cybersecurity Risk Manager, Cyber Legal, Policy and Compliance Officer (secondary);

6.2 Cybersecurity Management Fundamentals

Curator: RTU · **Level:** Advanced

Short description: This course focuses on methods, practices, and tools for an organisation's cybersecurity strategy management and implementation to ensure digital systems, services, and assets are protected. It thoroughly examines information security management processes, risk assessment, protection of corporate/personal data, digital identities, and the practical application of acquired knowledge.

Learning outcomes:

- Obtain knowledge and practical skills in cybersecurity governance, Common Cybersecurity Body of Knowledge, practices, processes, procedures, standards, certification, legal regulations, and ethics
- Promote abilities to select cybersecurity frameworks, methodologies, and standards
- Define business use for these frameworks and propose alternative solutions

Target ECSF Roles: Cybersecurity Risk Manager, Chief Information Security Officer (CISO) (primary); Cyber Legal, Policy and Compliance Officer (secondary);

6.3 Business Continuity and Digital Resilience

Curator: AaltoEE · **Level:** Beginner

Short description: Organisations are subjected to a variety of potential incidents that pose risks to their capabilities to continue operations. Companies and other organisations need to prepare for these so that they are well-positioned to continue business operations or get back operational quickly when incidents materialise. With the ever-increasing digitalisation, a crucial component in this business continuity planning is the resilience of key digital systems and tools. This course focuses on how to manage business continuity and digital resilience in modern organisations and discusses their key building blocks. It teaches how organisations can become more digitally resilient and prepared for different incidents that challenge their business continuity and how to manage them when they occur. This course is targeted at professionals and managers responsible for business continuity, risk management, IT, or digital operations who want to strengthen their organisation’s ability to withstand and recover from digital and operational disruptions.

Learning outcomes:

- Explain what business continuity and resilience mean in the context of digital organisations.
- Identify common threats to business continuity and resilience.
- Conduct preliminary business impact analysis of identified threats.
- Plan for business continuity and resilience.
- Draft an incident response and management plan.

Target ECSF Roles: Cybersecurity Risk Manager, Cyber Incident Responder (primary); Chief Information Security Officer (CISO) (secondary).

6.4 Risk Management for Organisations

Curator: LiU · **Level:** Intermediate

Short description: This course develops both theoretical knowledge and practical competence in cybersecurity risk management for organisations, closely integrating theory with hands-on practice. Students will build a solid grounding in risk management principles and strategies, gain familiarity with key industry standards and frameworks (such as ISO 27001 and the NIST Cybersecurity Framework), and develop practical experience with tools used for threat modelling and risk assessment. The course is structured in three parts: an introduction to the foundations of risk management, including the risk management lifecycle and relevant standards; a practical exploration of industry-recognised tools and techniques, supported by guided exercises; and an applied exercise in which students conduct a full risk management activity, either on a provided mock-up organisation or on material from their own professional setting.

Learning outcomes:

- Critically evaluate and apply cybersecurity risk management frameworks, methodologies, and standards to organisational contexts.
- Conduct a basic but structured risk assessment using appropriate tools, identifying and categorising threats, vulnerabilities, and their potential organisational impact.
- Select and justify suitable risk treatment strategies for identified risks, considering organisational priorities and risk appetite.
- Analyse and assess the cybersecurity risk of a real or realistic organisation, synthesising findings into a coherent risk management output.
- Communicate and present risk management findings clearly and effectively, demonstrating the ability to justify conclusions and respond to scrutiny.

Target ECSF Roles: Cybersecurity Risk Manager (primary); Chief Information Security Officer (CISO), Cybersecurity Auditor (secondary).

6.5 Information Security Management for Public Administration

Curator: KTH · **Level:** Intermediate

Short description: This course addresses information security and cybersecurity management as practised in public administration, with a focus on the governance, regulatory, and operational characteristics that distinguish public-sector cybersecurity from its private-sector counterpart. It covers cybersecurity as a strategic governance issue in public administration bodies, including the responsibilities, mandates, and decision-making structures that link political leadership to operational and IT functions; the legal and compliance framework specific to the public sector, including the principle of public disclosure, data protection, and the documentation and supervision requirements that public administration bodies must satisfy; the use of information classification and asset ownership as governance tools adapted to public administration contexts; the change-management practices required to translate cybersecurity decisions into operational reality across complex public-sector organisations, including communication with political and managerial leadership; the contemporary threat landscape facing public administration bodies; and the regulatory dimensions of cloud services and third-party dependencies in public-sector procurement, including supply-chain risk and cross-border data transfer obligations. The course is designed for cybersecurity managers, compliance officers, and IT security leaders working in or with public

administration bodies who need to translate generic information security frameworks into practices that fit the public-sector regulatory and governance context.

Learning outcomes:

- Identify the strategic governance responsibilities of a public administration body for information security and cybersecurity, including the division of responsibilities between political leadership, operational management, and IT and security functions.
- Apply the legal and regulatory framework specific to public administration, including public-disclosure and confidentiality requirements, data protection obligations, and the documentation and supervision regimes to which public bodies are subject.
- Use information classification and asset ownership as governance tools in a public administration context, integrating them into existing public-sector processes such as system administration, procurement, and change management.
- Plan and communicate cybersecurity-related organisational change across the political and administrative levels of a public administration body, including the framing of cybersecurity decisions for political leadership and the management of resistance.
- Recognise the contemporary threat landscape facing public administration bodies, including the principal threat actors and their objectives, and link technological threats to operational and reputational risks.
- Apply public-sector regulatory and contractual practices to the governance of cloud services and third-party providers, including supply-chain risk management and cross-border data transfer obligations.

Target ECSF Roles: Cyber Legal, Policy and Compliance Officer, Cybersecurity Auditor (primary); Chief Information Security Officer (CISO), Cybersecurity Risk Manager (secondary).

6.6 Cybersecurity for Journalists

Curator: RISE · **Level:** Mixed

Short description: The course provides practical cybersecurity training tailored to journalists, focusing on real-world threats, source protection and secure reporting practices. It combines foundational knowledge with hands-on guidance on secure communication, privacy and digital safety. Participants will explore the cybercrime landscape, common attack methods and techniques to remain secure in hostile digital environments. The course also addresses emerging risks, such as AI-generated misinformation, and includes essential legal and compliance considerations relevant to journalistic work in the EU context.

Learning outcomes:

- Understand key cybersecurity threats targeting journalists and common attack methods.
- Apply practical measures to secure communications, devices, and protect confidential sources.
- Apply basic security practices, assess AI-driven risks.
- Apply GDPR principles and the European Convention on Human Rights in daily work.

Target ECSF Roles: Not directly applicable. This course addresses the cybersecurity needs of journalists as

professional users of digital systems rather than as cybersecurity practitioners.

7. Foundations Pillar – Tier 4

Tier 4 of the Foundations pillar comprises four courses on transversal topics. Tier 4 courses are specialisations for trainees who have completed the relevant content in the other tiers and want to develop expertise in a transversal area that complements their primary Role. The courses are self-contained and can be taken independently of each other. Depending on the subject, Tier 4 courses are delivered synchronously, asynchronously, or in a blended format. Courses in this tier have a duration of 15 to 40 hours.

The following subsections describe each course in Tier 4. For each course, the subsection records the course title, the Curator partner, the level (beginner, intermediate, advanced, or mixed), a short description, and the course's learning outcomes.

7.1 Applied Cryptography

Curator: POLIMI · **Level:** Intermediate

Short description: This course provides a practical, use-case-driven introduction to applied cryptography. Rather than focusing on mathematical foundations, the course emphasises how cryptographic primitives and protocols are used correctly, and how they are commonly misused, in real-world systems. Participants will explore hash functions, symmetric and asymmetric encryption, digital signatures, and Public Key Infrastructure (PKI). They will see how these building blocks come together in protocols such as TLS, VPNs, and modern authentication mechanisms. Through concrete examples, demonstrations, and hands-on exercises, the course highlights typical pitfalls (such as the misuse of AES in ECB mode, insecure key management, or flawed JWT validation) and the correct patterns to adopt in their place. Additional topics include secure data storage, password hashing and multi-factor authentication, cryptographic aspects of blockchain, and the upcoming transition to post-quantum cryptography. By the end of the course, participants will be able to recognise cryptographic needs in their systems, select appropriate mechanisms, configure them correctly, and avoid the most common mistakes encountered in practice.

Learning outcomes:

- Explain the role and purpose of the main cryptographic primitives (hash functions, symmetric and asymmetric encryption, digital signatures) and identify appropriate use cases for each.
- Apply modern cryptographic algorithms correctly, including authenticated encryption, secure password hashing, and hybrid encryption schemes.
- Configure and manage PKI components, including certificates, certificate authorities, and trust chains.
- Deploy and troubleshoot TLS in real-world scenarios, recognising and correcting common misconfigurations.
- Implement secure authentication mechanisms, including multi-factor authentication and modern password less approaches (e.g., passkeys, WebAuthn).
- Apply sound key management practices, including secure key storage, rotation, and the use of secret management tools.
- Identify and avoid common cryptographic pitfalls, such as insecure modes of operation, nonce reuse, weak

password storage, and flawed token validation.

- Assess the cryptographic foundations of blockchain technologies and evaluate their suitability for specific use cases.
- Recognise the implications of the post-quantum transition and the importance of cryptographic agility in system design.

Target ECSF Roles: Cybersecurity Implementer (primary); Cybersecurity Architect (secondary);

7.2 Threat Modelling

Curator: POLIMI · **Level:** Intermediate

Short description: A course on threat modelling fundamentals covering system modelisation, threat identification, and risk evaluation strategies. The course introduces a structured approach to analysing complex systems, starting from the identification of assets, actors, and trust boundaries, and progressing toward the systematic discovery and evaluation of potential security and privacy threats. Participants learn to apply established methodologies such as STRIDE for security threat analysis and LINDDUN for privacy threat modelling, alongside the use of threat intelligence frameworks like MITRE ATT&CK to contextualise adversarial behaviours and techniques. Emphasis is placed on understanding both attacker perspectives and defensive design, enabling students to reason about threats in realistic and evolving environments. Through a hands-on group project, participants build a complete threat model for a chosen scenario. This includes the creation of Data Flow Diagrams (DFDs), detailed identification of assets and actors, definition of trust boundaries, structured threat elicitation, and risk assessment. Students also design and justify mitigation strategies, considering trade-offs between security, usability, and system performance. By the end of the course, students will be able to systematically analyse systems, identify and prioritise threats, and propose effective, context-aware mitigation measures aligned with industry best practices.

Learning outcomes:

- Systematically model complex systems using appropriate abstractions, including Data Flow Diagrams (DFDs), identifying assets, actors, and trust boundaries.
- Apply established threat modelling methodologies such as STRIDE, LINDDUN, and MITRE ATT&CK to identify security and privacy threats and associated scenarios.
- Identify, classify, and prioritise threats based on risk, likelihood, and potential impact.
- Collaborate effectively in a team to develop a comprehensive threat model for a real-world scenario.

Target ECSF Roles: Cybersecurity Architect, Cybersecurity Risk Manager (primary); Cyber Threat Intelligence Specialist, Penetration Tester (secondary).

7.3 AI for Cybersecurity

Curator: ULUS · **Level:** Mixed

Short description: This course bridges artificial intelligence and cybersecurity, equipping trainees with the knowledge and skills to use AI as a defensive tool for detecting, analysing, and responding to modern cyber threats. It introduces the AI-driven threat landscape and explores how machine learning can support intrusion

detection, anomaly detection, malware analysis, and security monitoring. Trainees will learn how AI-powered tools and analytics platforms can be used to identify suspicious activity, classify malware, analyse network traffic, and enhance threat intelligence. The course also covers AI-driven incident response, automated threat mitigation, compliance monitoring, and the ethical considerations involved in applying AI within cybersecurity environments. Designed for cybersecurity analysts, SOC personnel, network administrators, IT security managers, and compliance officers with basic cybersecurity familiarity, this course prepares trainees to apply AI techniques responsibly and effectively in modern security operations.

Learning outcomes:

- Detect network anomalies by applying machine learning-based techniques to a provided traffic log dataset, identifying at least three distinct anomalous patterns.
- Classify unknown malware samples using AI-driven behavioural analysis, correctly categorizing at least four out of five samples by threat type.
- Design an AI-assisted incident response workflow that specifies trigger conditions, automated mitigation steps, and human escalation points for a given attack scenario.
- Evaluate the effectiveness of an AI-driven threat intelligence feed by comparing its alert accuracy against a traditional signature-based system using a provided set of historical security events.
- Assess the ethical implications of deploying an AI cybersecurity tool by identifying at least two potential compliance risks and proposing corresponding safeguards.

Target ECSF Roles: Cyber Incident Responder, Cyber Threat Intelligence Specialist (primary); Cybersecurity Implementer (secondary);

7.4 Software Supply Chain Security

Curator: ELTE · **Level:** Advanced

Short description: This course covers the theory behind software supply chain attacks, from simple cases of typo squatting and dependency confusion to advanced compromise techniques targeting build systems, update mechanisms, and trusted third-party components. It explains how attackers exploit open-source ecosystems, package repositories, and developer workflows to introduce malicious code into otherwise legitimate software. The course also addresses the need for organisations to prepare for this growing threat through secure development practices, dependency governance, code signing, artefact integrity checks, and continuous monitoring. Participants will learn how to use free and open-source software more safely while reducing operational and security risk.

Learning outcomes:

- Identify supply chain security risks.
- Design safe CI/CD pipelines.
- Implement developer package policies.
- Evaluate open-source code risk.
- Analyse developer tool safety.

- Implement artefact repositories.

Target ECSF Roles: Cybersecurity Implementer, Cybersecurity Architect (primary); Cybersecurity Risk Manager (secondary).

8. Hands-On Pillar

The Hands-On pillar comprises five standalone practical courses in which trainees apply the Skills, Knowledge, and e-Competences acquired in the other pillars to realistic scenarios. The Hands-On pillar does not introduce new technical content: it is the capstone of the CYCERONE training experience, allowing trainees to validate their skills in a realistic, challenge-based, or simulated setting. Courses in this pillar are co-curated by all partners and coordinated by POLIMI. The duration of these courses is typically one full day, with the possibility of being extended to a second day.

The following subsections describe each course in the Hands-On pillar. For each course, the subsection records the goal of the practical experience.

8.1 Capture the Flag (CTF)

The CTF is a multi-category cybersecurity competition in which trainees solve challenges of increasing difficulty across several domains: binary exploitation, reverse engineering, web security, cloud security, digital forensics, and cryptanalysis. Challenges are designed so that solving them requires applying skills acquired in the Foundations pillar, particularly from the Tier 2 courses on Web Security, Cloud Security, Reverse Engineering and Binary Analysis, and Digital Forensics. Each challenge presents a realistic scenario in which the trainee must identify a vulnerability, exploit it, and retrieve a hidden flag that proves successful completion. The CTF format naturally fosters problem solving, time management, and, when played in teams, communication and collaborative decision-making.

8.2 Penetration Testing Lab

The Penetration Testing Lab is an open-ended practical exercise modelled on the HackTheBox format [15].

Trainees are given the IP addresses of one or more remote target machines and tasked with gaining access via a realistic attack chain. The exercise covers remote scanning for exposed services, brute force attacks, web application vulnerability discovery, lateral movement between compromised hosts, privilege escalation, exploitation of default configurations, and stealth scanning techniques. Unlike the CTF, which is structured around discrete challenges with clear flags, the Penetration Testing Lab requires trainees to plan and execute an end-to-end attack campaign, making decisions about which path to pursue and adapting their approach as they discover the target environment. The exercise develops the practical skills associated with the Penetration Tester and Cybersecurity Implementer Roles.

8.3 Secure Infrastructure Build-out

The Secure Infrastructure Build-out is an end-to-end exercise in which trainees construct a complete network and server infrastructure from scratch. The exercise proceeds through five stages: configuring a network switch, installing and configuring a Proxmox hypervisor (operating system, storage, networking) [16, 17], deploying a PFSense firewall with network access rules [18, 19], building and demonstrating an operational virtual machine cluster, and deploying AI-based systems on the infrastructure [31]. The exercise is designed to give trainees a

concrete understanding of how the security principles taught in the Tier 2 courses on Network and IoT Security and Cybersecurity Architecture translate into real infrastructure decisions.

8.4 DevSecOps Pipeline Simulation

The DevSecOps Pipeline Simulation is a guided exercise in which trainees build a complete secure CI/CD pipeline from scratch [28, 29]. The exercise is structured in four phases. In the first phase, trainees set up a virtual machine environment, install version control (Git) [20], a web application server, and configure the initial deployment. In the second phase, they integrate security tools into the pipeline: SonarQube for static application security testing [22], Trivy for container and file system scanning [23, 24], and Snyk for software composition analysis [25]. In the third phase, they configure Jenkins as the automation server and implement automated security gates that block deployment when vulnerabilities are detected [21]. In the fourth phase, trainees generate a software bill of materials (SBOM) using CycloneDX [26, 27] and map the pipeline artefacts to the relevant articles of the Cyber Resilience Act [14], and to the SLSA supply-chain integrity framework [30], producing a compliance report.

8.5 Incident Response Crisis Simulation

The Incident Response Crisis Simulation is a role-based exercise in which trainees experience a simulated data breach unfolding across six escalating phases. In the first phase, a zero-day vulnerability appears in the news. In the second phase, the vulnerability is used to breach the case company; the extent of the damage is not yet known. In the third phase, the attackers begin blackmailing the company. In the fourth phase, the breach is discovered to affect the personal data of most of the company's customers. In the fifth phase, the attackers publish a sample of the stolen data. In the sixth phase, the breach becomes a news story, and the company faces public scrutiny.

Trainees are assigned roles that reflect the different professional perspectives involved in a real crisis: the incident response team, the data protection officer, the legal counsel, the management team, and the communications function. The exercise integrates technical incident response, including identifying the attack vector, containing the breach, and restoring operations, in line with recognised incident handling and incident management guidance [32, 33]. It also incorporates GDPR breach notification obligations, including assessing the severity of the breach, notifying the competent supervisory authority within 72 hours where required, and communicating with affected data subjects when the breach is likely to result in a high risk to their rights and freedoms [8, 34]. In addition, the simulation includes crisis management activities such as internal coordination, external communication, and media handling, reflecting the organisational and cross-functional nature of major cybersecurity incidents.

As this Hands-on activity is being developed specifically for CYCERONE, its final scope and structure will be refined during the implementation phase. The current design foresees an exercise that can involve both technical and management-oriented audiences, but the exact roles, scenarios, and balance between technical response and organisational decision-making may be adjusted before delivery.

9. ECSF Role Coverage and Learning Paths

This section analyses the catalogue from two perspectives: how well the courses in the catalogue support each ECSF Role, and how effectively the courses are organised into learning paths to guide trainees toward the level of competence required by their target Role.

9.1 ECSF Role Coverage

The following analysis lists each of the twelve ECSF Roles defined in [1] and identifies the courses in the catalogue that contribute to its formation. A course contributes to a Role when its Skills, Knowledge, and e-Competences overlap with those listed in the ECSF Role profile for that Role.

- **Cybersecurity Implementer.** This is the most broadly covered Role in the catalogue, reflecting its position as the most demanded Role in the D4.4 Skills Gap Analysis. Tier 2 courses addressing this Role include Web Security (UNITN), Cloud Security (UNITN), Network and IoT Security (UBB), Security Orchestration and Automation (NTUA), Software Safety and Security (KTH), and Secure Software Development (TAU). Tier 4 contributes Applied Cryptography (POLIMI) and Software Supply Chain Security (ELTE), which support secure implementation practices across different technical domains. The Hands-On pillar adds the Secure Infrastructure Build-out and the DevSecOps Pipeline Simulation.

- **Penetration Tester.** Tier 2 courses addressing this Role include Web Security (UNITN), Cloud Security (UNITN), Reverse Engineering and Binary Analysis (POLIMI), and Software Safety and Security (KTH). Secure Software Development (TAU) also contributes as a secondary course, particularly for understanding secure coding practices from an attacker-aware perspective. Tier 4 contributes Threat Modelling (POLIMI), which provides the methodological dimension of attack surface analysis. The Hands-On pillar adds the CTF and the Penetration Testing Lab.

- **Digital Forensics Investigator.** Tier 2 courses addressing this Role include Digital Forensics (RTU) and Reverse Engineering and Binary Analysis (POLIMI), which covers the malware analysis component. The Hands-On pillar adds the CTF, which includes forensics challenges.

- **Cyber Incident Responder.** Tier 2 courses addressing this Role include Reverse Engineering and Binary Analysis (POLIMI), Digital Forensics (RTU), and Security Orchestration and Automation (NTUA). Tier 3 contributes Business Continuity and Digital Resilience (AaltoEE), which addresses organisational preparedness, continuity planning, and recovery in the context of cybersecurity and operational incidents. Tier 4 contributes AI for Cybersecurity (ULUS), which supports detection, analysis, and AI-assisted response to cyber threats. The Hands-On pillar adds the Incident Response Crisis Simulation.

- **Cybersecurity Architect.** Tier 1 contributes Privacy Foundations (ULUS), which addresses privacy engineering, privacy-by-design, and privacy requirements across the system lifecycle. Tier 2 courses addressing this Role include Cybersecurity Architecture (RTU) and Software Safety and Security (KTH). Tier 4 contributes Applied Cryptography (POLIMI), Threat Modelling (POLIMI), and Software Supply Chain Security (ELTE). The Hands-On pillar adds the Secure Infrastructure Build-out.

- **Cyber Threat Intelligence Specialist.** This Role receives more selective coverage than the core operational and management Roles prioritised for the CYCERONE target audience. Tier 2 courses addressing it include Reverse Engineering and Binary Analysis (POLIMI), which supports malware and binary analysis, and Digital Forensics (RTU), which contributes to evidence analysis and threat detection. Tier 4 contributes AI for Cybersecurity (ULUS), which addresses AI-supported threat detection, analysis, and intelligence workflows, and Threat Modelling (POLIMI), which provides a structured approach to adversarial behaviour and attack scenarios. The Hands-On pillar adds the Incident Response Crisis Simulation.

- **CISO.** Tier 3 courses addressing this Role include Cybersecurity for Management (RISE), Cybersecurity Management Fundamentals (RTU), Business Continuity and Digital Resilience (AaltoEE), Risk Management for Organisations (LiU), and Information Security Management for Public Administration (KTH). Tier 1 Privacy Foundations (ULUS) also contributes by addressing privacy governance and privacy-by-design from an organisational perspective. The Hands-On pillar adds the Incident Response Crisis Simulation, which gives CISOs practical experience of managing a crisis from a leadership position.

- **Cybersecurity Risk Manager.** Tier 1 contributes Privacy Foundations (ULUS), which addresses privacy

governance and privacy-related risk management. Tier 3 courses addressing this Role include Cybersecurity for Management (RISE), Cybersecurity Management Fundamentals (RTU), Business Continuity and Digital Resilience (AaltoEE), and Risk Management for Organisations (LiU). Tier 4 contributes Threat Modelling (POLIMI), which provides an analytical method for identifying and prioritising risks, and Software Supply Chain Security (ELTE), which addresses risks associated with dependencies, development workflows, and third-party software components. The Hands-On pillar adds the Incident Response Crisis Simulation, which addresses risk-related crisis response from a management perspective.

- **Cybersecurity Auditor.** Tier 3 courses addressing this Role include Cybersecurity Management Fundamentals (RTU), Risk Management for Organisations (LiU), and Information Security Management for Public Administration (KTH). These courses support the governance, risk assessment, control, and organisational-resilience dimensions of audit work; the public-administration course in particular addresses the documentation, supervision, and audit-readiness practices that public-sector auditors encounter.

- **Cyber Legal, Policy and Compliance Officer.** Awareness-level Security Compliance (AaltoEE) provides an introductory basis for understanding regulatory and compliance-related cybersecurity issues. Tier 1 Privacy Foundations (ULUS) contributes privacy governance, privacy engineering, and data-protection principles. Tier 3 courses addressing this Role include Cybersecurity for Management (RISE) and Cybersecurity Management Fundamentals (RTU). Information Security Management for Public Administration (KTH) is the principal Tier 3 contribution to this Role, addressing public-sector regulatory frameworks, public-disclosure and confidentiality obligations, and the supervision and documentation regimes that compliance officers must satisfy in public administration bodies. Cybersecurity for Journalists (RISE) provides a complementary sector-specific perspective. Tier 4 contributes Software Supply Chain Security (ELTE), which addresses supply-chain-related regulatory and organisational obligations. The Hands-On pillar adds the Incident Response Crisis Simulation, which covers breach management and notification responsibilities.

- **Cybersecurity Educator.** All eight Awareness pillar courses are educator-oriented by nature. Tier 1 Social Engineering (ELTE) also contributes, as it is designed to be delivered by educators across partner institutions.

- **Cybersecurity Researcher.** Tier 2 contributes Reverse Engineering and Binary Analysis (POLIMI), which supports malware analysis, binary inspection, and advanced technical investigation, and Software Safety and Security (KTH), which covers formal methods and research-grade verification tools. Tier 4 contributes AI for Cybersecurity (ULUS), which addresses AI-supported detection and analysis at the boundary between professional practice and emerging research. Applied Cryptography (POLIMI) may also support research-oriented trainees whose work involves cryptographic mechanisms, although its primary catalogue mapping is to implementation and architecture Roles.

9.2 Relevance of ECSF Roles to the Target Audience

The analysis above confirms the intermediate catalogue provides coverage for all twelve ECSF Roles. However, not all twelve Roles carry the same weight for the CYCERONE target audience. The ECSF was designed as a comprehensive taxonomy of the cybersecurity profession, covering the full spectrum, from operational practice to academic research and from technical execution to strategic governance. The CYCERONE target audience, by contrast, consists specifically of professionals working in SMEs and public administration bodies, which narrows the set of Roles that are of primary practical relevance.

Some Roles are central to this audience. The Cybersecurity Implementer is the most immediately needed Role in

any SME or public administration: the professional who configures, deploys, and maintains the security of systems and services. The CISO and the Cybersecurity Risk Manager are essential in every organisation that must comply with NIS2 or manage cybersecurity governance, even when the role is held part-time or combined with other responsibilities. The Cyber Incident Responder is equally relevant: every organisation must be able to detect, contain, and recover from incidents, and SMEs often lack the internal capacity to do so.

Other Roles are relevant but are more commonly exercised by external service providers rather than by in-house staff. The Penetration Tester and the Digital Forensics Investigator, for example, are Roles that SMEs typically access through outsourcing arrangements: an SME is more likely to contract a penetration test from a specialised firm than to employ a full-time penetration tester. Nevertheless, training SME professionals in these areas remains valuable because it enables them to understand, commission, and evaluate the work of external specialists, and because some larger SMEs and public administration bodies do maintain in-house capabilities in these areas. A similar observation applies to the Cybersecurity Auditor, whose function in smaller organisations is often performed by the compliance officer or by an external auditor rather than by a dedicated cybersecurity audit professional.

The Cyber Threat Intelligence Specialist is a Role that is primarily found in large organisations, sectoral and national CSIRTs, and specialised threat intelligence firms. It is not a Role that most SMEs or public administration bodies would staff internally. The catalogue's relatively thin coverage of this Role is therefore consistent with the priorities of the target audience, rather than a gap that requires urgent attention.

Two Roles occupy a distinct position in the ECSF taxonomy. The Cybersecurity Educator is a meta-Role: it describes the professional who trains others in cybersecurity, rather than a professional who practises cybersecurity directly. For CYCERONE, this Role is addressed implicitly through the Awareness pillar, which produces the content that educators deliver, and through the co-creation model in which partner instructors learn to deliver each other's material. The Cybersecurity Researcher is an academic and R&D Role that is not part of the typical workforce profile of an SME or public administration body. The catalogue covers it through the Tier 2 Software Safety and Security course (KTH) and the Tier 4 Applied Cryptography and AI for Cybersecurity courses, which operate at the boundary between professional practice and active research. The consortium is confident this level of coverage is appropriate since CYCERONE is a training programme for practitioners, not a research capacity-building initiative.

In summary, the catalogue's coverage is strongest precisely where the target audience's needs are greatest, and thinner where the Roles are less likely to be exercised in-house by SME and public administration professionals. This is a deliberate prioritisation choice, aligned with the evidence collected in D4.4 and with the objective of building a catalogue that responds to the most relevant training needs of the CYCERONE target groups.

9.3 Learning Paths

The catalogue is designed to support learning paths that guide trainees from foundational knowledge to the level of competence required by their target ECSF Role. A learning path is an ordered sequence of courses, typically spanning two or three pillars, that a trainee follows to acquire the Skills, Knowledge, and e-Competences associated with a specific Role.

At the intermediate stage of the catalogue, the consortium has identified learning paths for 10 ECSF Roles. These paths prioritise the Roles most relevant to the CYCERONE target audience, as identified in the D4.4 Skills Gap Analysis, while also including selected reference paths for more specialised Roles. In particular, Roles such as Cybersecurity Implementer, CISO, Cybersecurity Risk Manager, Cyber Incident Responder, and Cyber Legal, Policy and Compliance Officer are central to the needs of SMEs and public administration bodies. By contrast, paths such as Digital Forensics Investigator and Cyber Threat Intelligence Specialist are included as indicative reference paths: they demonstrate the catalogue’s coverage of more specialised profiles, while recognising that these Roles

may be less commonly exercised in-house by the target organisations.

- **Penetration Tester.** A trainee targeting the Penetration Tester Role would begin with baseline cybersecurity literacy and applied security practice, then progress to technical courses focused on vulnerability discovery, exploitation, and attack-surface analysis. The path culminates in practical challenge-based activities.

  Recommended path: Cybersecurity Awareness → Applied Cybersecurity → Web Security → Cloud Security → Reverse Engineering and Binary Analysis → Threat Modelling → Capture the Flag (CTF) → Penetration Testing Lab

- **Cybersecurity Implementer.** A trainee targeting the Cybersecurity Implementer Role would begin with general cybersecurity awareness and applied security practice, then progress to courses focused on securing networks, systems, software, and operational environments. The path may be complemented with specialised courses on cryptography, supply chain security, and AI-enabled security operations.

  Recommended path: Cybersecurity Awareness → Cybersecurity for Everyone → Applied Cybersecurity → Network and IoT Security → Security Orchestration and Automation → Secure Software Development → Applied Cryptography → Software Supply Chain Security → Secure Infrastructure Build-out → DevSecOps Pipeline Simulation

- **Chief Information Security Officer (CISO).** A trainee targeting the CISO Role would follow a management- and governance-oriented path. The path begins with awareness-level courses on risk, compliance, and privacy, then progresses to strategic courses addressing cybersecurity governance, management, resilience, and organisational decision-making. For this Role, the Hands-On component is limited to crisis-management simulation rather than technical execution.

  Recommended path: Risk Management Fundamentals → Security Compliance → Privacy Foundations → Cybersecurity for Management → Cybersecurity Management Fundamentals → Business Continuity and Digital Resilience → Risk Management for Organisations → Information Security Management for Public Administration → Incident Response Crisis Simulation

- **Cybersecurity Risk Manager.** A trainee targeting the Cybersecurity Risk Manager Role would begin with introductory risk and compliance concepts, then progress to structured risk management, continuity planning, privacy governance, and threat modelling. The path is designed to support professionals who assess, prioritise, and communicate cybersecurity risks in organisational contexts.

  Recommended path: Risk Management Fundamentals → Security Compliance → Privacy Foundations → Cybersecurity Management Fundamentals → Business Continuity and Digital Resilience → Risk Management for Organisations → Threat Modelling → Incident Response Crisis Simulation

- **Cyber Incident Responder.** A trainee targeting the Cyber Incident Responder Role would begin with general cybersecurity awareness and digital-forensics readiness, then progress to technical and organisational courses covering investigation, orchestration, automation, resilience, and incident management. The path culminates in simulation-based exercises that require coordinated technical and organisational response.

  Recommended path: Cybersecurity Awareness → Digital Forensics Fundamentals → Applied Cybersecurity → Digital Forensics → Security Orchestration and Automation → Reverse Engineering and Binary Analysis → Business Continuity and Digital Resilience → AI for Cybersecurity → Incident Response Crisis Simulation

- **Cybersecurity Architect.** A trainee targeting the Cybersecurity Architect Role would progress from general cybersecurity awareness to technical courses on system design, architecture, secure networks, formal methods, privacy engineering, cryptography, and threat modelling. The path culminates in infrastructure-oriented practical work.

  Recommended path: Cybersecurity Awareness → Privacy Foundations → Network and IoT Security → Cybersecurity Architecture → Software Safety and Security → Applied Cryptography → Threat Modelling → Software Supply Chain Security → Secure Infrastructure Build-out

- **Cyber Legal, Policy and Compliance Officer.** A trainee targeting the Cyber Legal, Policy and Compliance Officer Role would follow a non-technical path focused on privacy, compliance, governance, organisational resilience, and regulatory obligations. This path is particularly relevant for public administration bodies and SMEs where legal, compliance, and security responsibilities may be combined.

  Recommended path: Privacy → Security Compliance → Privacy Foundations → Cybersecurity for Management → Cybersecurity Management Fundamentals → Business Continuity and Digital Resilience → Information Security Management for Public Administration → Software Supply Chain Security → Incident Response Crisis Simulation

- **Cybersecurity Auditor.** A trainee targeting the Cybersecurity Auditor Role would follow a governance-, risk-, and compliance-oriented path. The path begins with awareness-level compliance and risk concepts, then progresses to cybersecurity management, organisational risk assessment, control evaluation, and information security management in public-sector or organisational contexts. The path is designed to support professionals who assess whether cybersecurity policies, controls, and practices are appropriate, documented, and effectively implemented.

  Recommended path: Security Compliance → Risk Management Fundamentals → Cybersecurity Management Fundamentals → Risk Management for Organisations → Information Security Management for Public Administration

- **Digital Forensics Investigator.** A trainee targeting the Digital Forensics Investigator Role would begin with non-specialist forensic awareness, then progress to technical investigation, malware analysis, and evidence-handling competences. The path culminates in practical exercises involving forensic or reverse-engineering challenges.

  Recommended path: Digital Forensics Fundamentals → Applied Cybersecurity → Digital Forensics → Reverse Engineering and Binary Analysis → Security Orchestration and Automation → Capture the Flag (CTF) → Incident Response Crisis Simulation

- **Cyber Threat Intelligence Specialist.** A trainee targeting the Cyber Threat Intelligence Specialist Role would follow a selective technical path focused on detection, analysis, automation, malware understanding, and AI-supported threat analysis. This path is included as an intermediate reference path, while recognising that the Role is more commonly found in larger organisations, CSIRTs, and specialised providers.

  Recommended path: Cybersecurity Awareness → Social Engineering → Security Orchestration and Automation → Reverse Engineering and Binary Analysis → Digital Forensics → AI for Cybersecurity → Threat Modelling → Incident Response Crisis Simulation

The Role-based paths above are organised around ECSF Role profiles and therefore describe progression toward recognised cybersecurity professional functions. However, the consortium also recognises that professionals in SMEs and public administration bodies do not always identify with, or operate within, a single ECSF Role. In

smaller organisations, cybersecurity responsibilities are often combined with other organisational, technical, legal, or managerial duties. A compliance officer in a municipality, a system administrator in an SME who also supports incident response, or a software developer responsible for integrating security into the development pipeline may all require training that cuts across several ECSF Roles. For this reason, the catalogue can also support cross-functional learning paths. These paths do not replace the ECSF Role-based paths; rather, they translate the catalogue into practical training journeys that reflect how cybersecurity responsibilities are commonly distributed in SMEs and public administration bodies.

- **Secure Software and DevSecOps Profile.** This path targets developers, software engineers, IT staff, and technical managers responsible for integrating security into software development and deployment processes. It combines application security, cloud security, secure development, software verification, cryptographic mechanisms, supply-chain security, and practical DevSecOps implementation.

  Recommended path: Cybersecurity Awareness → Applied Cybersecurity → Web Security → Cloud Security → Secure Software Development → Software Safety and Security → Applied Cryptography → Software Supply Chain Security → DevSecOps Pipeline Simulation

- **SME Cybersecurity Responsible.** This path targets professionals in SMEs who are not full-time cybersecurity specialists but are responsible for coordinating cybersecurity activities, selecting or liaising with external providers, supporting compliance, managing basic risk processes, and improving organisational resilience.

  Recommended path: Cybersecurity Awareness → Privacy → Risk Management Fundamentals → Security Compliance → Cybersecurity for Everyone → Applied Cybersecurity → Cybersecurity for Management → Business Continuity and Digital Resilience → Risk Management for Organisations → Incident Response Crisis Simulation

- **Public Administration Security and Compliance Profile.** This path targets professionals in public administration bodies whose responsibilities combine cybersecurity awareness, privacy, compliance, continuity planning, organisational resilience, and incident coordination. It is designed for contexts where cybersecurity is closely linked to regulatory obligations, public-service continuity, procurement, and communication with citizens or external stakeholders. The Incident Response Crisis Simulation provides the practical component of the path, as it allows trainees to apply coordination, communication, and breach-management responsibilities in a realistic organisational setting.

  Recommended path: Cybersecurity Awareness → Privacy → Security Compliance → Privacy Foundations → Cybersecurity for Management → Cybersecurity Management Fundamentals → Business Continuity and Digital Resilience → Information Security Management for Public Administration → Incident Response Crisis Simulation

Between M16 and M36, the consortium will explore the feasibility of additional learning paths tailored to these concrete professional figures, combining courses from different tiers and pillars into progressions that reflect the way cybersecurity responsibilities are actually distributed in smaller organisations.

10. Conclusions

This deliverable has presented the intermediate version of the CYCERONE course catalogue, consisting of thirty-six courses organised across the Awareness, Foundations, and Hands-On pillars. As the companion to D3.6, which defines the educational architecture and course format of the CYCERONE training offering, D4.5 documents how that architecture is populated at month 16 with concrete courses, partner responsibilities, role coverage, and indicative learning paths.

The catalogue represents a harmonised intermediate offer rather than a simple aggregation of partner courses. Starting from the 48-course baseline defined in the Grant Agreement and the educational assets available across the consortium, the catalogue was consolidated into a more focused structure aligned with the ECSF, the e-CF, the three-pillar architecture, and the needs identified through the D4.4 Skills Gap Analysis. This process allowed overlapping material to be merged or re-scoped, less directly relevant entries to be excluded from the intermediate version, and existing partner material to be adapted to the CYCERONE pedagogical model.

The resulting catalogue provides broad coverage of the twelve ECSF Roles while prioritising those that are most relevant to the CYCERONE target audience. Roles that are more likely to be performed internally by SMEs and public administration bodies, such as Cybersecurity Implementer, CISO, Cybersecurity Risk Manager, and Cyber Incident Responder, receive stronger and more structured coverage. Roles that are more commonly outsourced, performed by specialised providers, or associated with larger organisations, such as Cyber Threat Intelligence Specialist, Cybersecurity Auditor, Cybersecurity Researcher, and some aspects of Digital Forensics and Penetration Testing, are covered more selectively. This distribution is a deliberate design choice: the catalogue is intended to respond first to the most immediate and realistic training needs of the project's target groups, while still ensuring that all ECSF Roles are represented.

The learning paths presented in Section 9.3 show how the catalogue can support structured progression from baseline awareness to role-oriented competence and, where appropriate, to practical application through Hands-on activities. At the same time, the catalogue recognises that professionals in SMEs and public administration do not always correspond neatly to a single ECSF Role. For this reason, the role-based paths presented in this intermediate version should be understood as indicative reference paths, to be refined and complemented during the second half of the project with pathways that better reflect combined responsibilities in smaller organisations.

As an intermediate deliverable, the catalogue is not final. Between M18 and M36, the delivery of the courses will generate evidence from actual implementation, including feedback from trainees, instructors, course curators, and partner organisations. This evidence will be used to assess whether individual courses require minor adjustments, substantial redesign, replacement, or integration with additional material. It will also support the refinement of learning paths, the validation of course relevance, and the possible introduction of new content in response to emerging technologies, regulatory developments, or changing training needs.

The final version of the catalogue, to be delivered in D4.2 at M36, will therefore build on both the methodological consolidation described in this deliverable and the lessons learned from course delivery. Its objective will be to provide a validated, improved, and sustainable CYCERONE training offer that remains coherent with the project's educational architecture while responding to the practical cybersecurity needs of SMEs and public administration professionals.

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

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

[6] 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.

[7] 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.

[8] 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.

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

[10] CYCERONE Consortium, *D4.4 — Skills Gap Report (Intermediate Version)*, Lead: RTU, M16, 2026.

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

[12] CYCERONE Consortium, *D3.6 — CYCERONE Platform Concept and Course Format Offering (Intermediate Version)*, Lead: POLIMI, M16, 2026 (companion deliverable).

[13] 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.

[14] 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.

[15] Hack The Box Ltd., *Hack The Box — Cybersecurity Training Platform, 2017*. https://www.hackthebox.com/

[16] Proxmox Server Solutions GmbH, *Proxmox Virtual Environment Documentation*. Available: https://pve.proxmox.com/pve-docs/pve-admin-guide.html

[17] Proxmox Server Solutions GmbH, *Proxmox VE Administration Guide*. Available: https://pve.proxmox.com/pve-docs/pve-admin-guide.html

[18] Netgate, *pfSense Documentation*. Available: https://docs.netgate.com/pfsense/en/latest/

[19] Netgate, *pfSense Documentation — Firewall*. Available: https://docs.netgate.com/pfsense/en/latest/firewall/index.html

[20] Software Freedom Conservancy, *Git Documentation*. Available: https://git-scm.com/docs/git

[21] Jenkins Project, *Jenkins User Documentation*. Available: https://www.jenkins.io/doc/

[22] SonarSource, *SonarQube Server Documentation*. Available: https://docs.sonarsource.com/sonarqube-server/

[23] Aqua Security, *Trivy Documentation*. Available: https://trivy.dev/docs/

[24] Aqua Security, *Trivy — Vulnerability Scanning*. Available: https://trivy.dev/docs/latest/scanner/vulnerability/

[25] Snyk Ltd., *Software Composition Analysis (SCA)*. Available: https://snyk.io/articles/open-source-security/software-composition-analysis-sca/

[26] OWASP Foundation, *CycloneDX Bill of Materials Standard*. Available: https://cyclonedx.org/

[27] OWASP Foundation, *CycloneDX Specification Overview*. Available: https://cyclonedx.org/specification/overview/

[28] OWASP Foundation, *OWASP DevSecOps Guideline*. Available: https://owasp.org/www-project-devsecops-guideline/

[29] OWASP Foundation, *OWASP Top 10 CI/CD Security Risks*. Available: https://owasp.org/www-project-top-10-ci-cd-security-risks/

[30] Open Source Security Foundation, *SLSA — Supply-chain Levels for Software Artifacts*. Available: https://slsa.dev/

[31] NIST, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, National Institute of Standards and Technology, January 2023. Available: https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10

[32] NIST, *Computer Security Incident Handling Guide*, Special Publication 800-61 Revision 2, National Institute of Standards and Technology, August 2012. Available: https://csrc.nist.gov/pubs/sp/800/61/r2/final

[33] ENISA, Good Practice Guide for Incident Management, European Union Agency for Cybersecurity, December 2010. Available: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[34] European Data Protection Board, Guidelines 9/2022 on Personal Data Breach Notification under GDPR, Version 2.0, 4 April 2023. Available: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en