DIGITAL-ECCC-2022-CYBER-B-03-SOC
DIGITAL JU Simple Grants
Grant Agreement No.: 101145874

Next Generation Security Operation Centres

D5.1 Skills development strategy report			
Report Identifier:	D5.1		
Work-package:	WP5	**Task:**	T5.1
Responsible Partner:	University of Piraeus Research Center (UPRC)	**Version Number:**	1.0
Due Date	31/12/2024	**Document Date:**	24/01/2025
Distribution Security:	PUB	**Deliverable Type:**	R
Keywords:	Skills development, cybersecurity training		
Project website: https://ng-soc.eu/			

Document History

Version	Content & Changes	Issue Date
0.1	**Document created**	**1/10/2024**
0.2	**Document sent for review**	**20/12/2024**
0.3	**Document reviewed**	**09/01/2025**
0.4	**Document reviewed**	**13/01/2025**
0.5	**Reviews are combined**	**13/01/2025**
0.6	**Sent for Quality Assurance**	**13/01/2025**
0.7	**Remarks from QA Consolidated**	**24/01/2025**
1.0	**Submission**	**24/01/2025**

Quality Control

	Name	Organisation	Date
Editor	Costas Lambrinoudakis	University of Piraeus Research Centre	20/12/2024
Peer review 1	Apostolos Gkletos	European Dynamics Greece	09/01/2025
Peer review 2	Stefanos Andreou	Cyprus Research and Academic Network	13/01/2025
Authorised by (Technical Coordinator)	Vasileios Mavroeidis	Cyentific	15/01/2025
Authorised by (Quality Manager)	Themis Kolyvas	European Dynamics Greece	24/01/2025
Submitted by (Project Coordinator)	Anastasia Garbi	European Dynamics	24/01/2025

Legal Disclaimer

NG-SOC is an EU project funded by the Digital Europe Programme (DIGITAL) under grant agreement No. 101145874. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The NG-SOC Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Table of Contents

List of Figures

List of Tables

Abbreviations

Acronym	Description
CMM	Capacity Maturity Model
DoW	Description of Work
EU	European Union
EC	European Commission
ECSF	European Cybersecurity Skills Framework
ECSO	European Cyber Security Organisation
GA	Grant Agreement
IDEB	Innovation, Dissemination & Exploitation Board
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
PC	Project Coordinator
PEB	Project Executive Board
PMI	Project Management Institute
PGA	Project General Assembly
QAS	Quality Assurance Supervisor
QMP	Quality Management Plan
SW, S/W	Software
TL	Task Leader
WP	Work Package
WPL	Work Package Leader

Executive Summary

This deliverable, developed under Work Package 5 (WP5), outlines a coherent strategy to advance Europe's cybersecurity workforce. Building on prior project results and aligning with established European frameworks such as the European Cybersecurity Skills Framework (ECSF) and ECSO's Minimum Reference Curriculum, it identifies critical knowledge areas while fostering proactive organizational engagement in skill development.

At its core, Task 5.1 defines a strategic approach to workforce skill enhancement. By examining training policies, organizational strategies, and methods to support both emerging and experienced professionals, this task establishes a foundation for sustainable workforce resilience. Key outcomes include addressing existing gaps in training and proposing innovative approaches to equip non-traditional entrants and enhance overall capacity.

In addition, Task 5.1 directly informs subsequent efforts within WP5. Specifically, the strategic insights feed into Task 5.2, which focuses on developing a scalable and flexible educational platform. This platform will leverage virtualization and cyber range technologies to deliver immersive, hands-on training scenarios, ensuring the practical application of the strategies identified in Task 5.1.

The findings from Task 5.1 also play a pivotal role in Task 5.3, shaping the design of realistic training and exercise scenarios. By highlighting gaps in existing approaches and emphasizing the importance of workplace innovation, Task 5.1 provides a thematic and technical framework for crafting inclusive, impactful training content. For example, its focus on real-world scenario training and the role of employers in upskilling individuals from diverse backgrounds ensures that these scenarios meet the dynamic needs of the cybersecurity workforce.

In summary, the efforts under WP5 seamlessly connect strategic planning with practical training solutions, ensuring Europe's cybersecurity workforce is well-prepared to adapt to evolving challenges and sustain robust defense capabilities.

1 Introduction

This deliverable is produced under Work Package 5 (WP5), which focuses on enhancing the overall capability and resilience of the cybersecurity workforce. It builds upon insights and outcomes from previous work packages and leverages established European cybersecurity skill development frameworks. The primary objective at this stage is to formulate a comprehensive strategy that not only identifies key cybersecurity knowledge areas but also encourages organizations to actively engage in nurturing a skilled and adaptable cybersecurity talent pool.

Within WP5, the tasks are structured to address both strategic and practical dimensions of workforce development:

- **T5.1 Strategy for Skills Development of Cybersecurity Professionals:** The present deliverable concentrates on the outcomes of T5.1, where a strategy for workforce skills development is established. This strategy builds upon existing references such as the European Cybersecurity Skills Framework (ECSF) by ENISA and the Minimum Reference Curriculum by ECSO**.** These frameworks inform a structured, holistic approach to strengthening cybersecurity capabilities within organizations, considering strategic, operational, technical, legal, and cultural aspects. T5.1 also examines training policies, workplace innovation, and the responsibility of employers to equip both newcomers and seasoned professionals with the necessary cybersecurity competencies.
- **T5.2 Hands-On Educational Platform:** Although this deliverable does not cover T5.2 in detail, it is introduced here as the next step in our holistic training approach. Future work will focus on using a scalable and flexible platform that integrates virtualization and cyber range technologies to provide interactive, real-world training scenarios. This platform, to be elaborated in subsequent deliverable, will reinforce the strategic foundations laid in T5.1 by offering cost-effective, repeatable, and engaging hands-on training experiences.
- **T5.3 Development of Realistic Cybersecurity Training and Exercise Scenarios:** Task 5.3 complements the work done in T5.1 and T5.2 by focusing on the creation of realistic, adaptable training and exercise scenarios. These scenarios, based on the strategic insights from T5.1, leverage the technological capabilities of the educational platform developed in T5.2. The outputs of T5.3 aim to provide immersive, scenario-based training experiences tailored to organizational needs, enabling trainees to engage with real-world challenges in a controlled and scalable environment.

By first establishing a robust strategic framework (T5.1), subsequently implementing a cutting-edge training platform (T5.2) and finally crafting realistic training scenarios (T5.3), WP5 aims to deliver a cohesive approach to cybersecurity skills development. This introduction sets the stage for the present deliverable, which delves into the strategic insights and recommendations emerging from T5.1.

1.1 Overview

This deliverable encompasses the development of a comprehensive strategy for the skills development of the cybersecurity workforce. The strategy is designed to extend beyond mere policy formulation by encouraging organizations to take an active role in cultivating a national cybersecurity workforce. Key components of the strategy include:

- **Identification of Existing Gaps and Barriers:** An analysis of current deficiencies in cybersecurity skills and the obstacles hindering workforce development.
- **Proposed Skill Development Approach:** A recommended methodology aimed at bridging identified gaps, including training schemes, workplace innovation policies, and retention strategies.
- **Integration with Established Frameworks:** Leveraging existing resources such as the European Cybersecurity Skills Framework (ECSF) from ENISA, and the Minimum Reference Curriculum from ECSO to inform and enhance the strategy.
- **Training and Retention Initiatives:** Investigation into effective training schemes and policies that facilitate the entry and retention of cybersecurity professionals, including discussions on employer responsibilities in training individuals without prior cybersecurity backgrounds.

The objectives related to this deliverable have been achieved in full and as scheduled.

1.2 Deliverable Structure

The deliverable is structured in five (5) chapters:

- Chapter 1 is the introduction of the document.
- Chapter 2 provides an overview of skills development and capacity building frameworks focusing on the ECSF and the ECSO minimum curriculum
- Chapter 3 entails the proposed skills development approach
- Chapter 4 demonstrates the alignment of the modular approach that was recommended for the skills development training program with the ECSO minimum curriculum.
- Chapter 5 draws conclusions.

2 Skills Development and Capacity Building Frameworks

2.1 ECSF methodology

The European Cybersecurity Skills Framework (ECSF) is designed to address the growing need for cybersecurity professionals by offering a structured approach to defining roles, competencies, and proficiency levels. Its primary goal is to harmonize skill sets and career pathways while ensuring adaptability to technological advancements and evolving industry requirements. According to the European Union Agency for Cybersecurity (ENISA), the current lack of a unified understanding of Europe's cybersecurity workforce and its associated skill sets impedes the development of standardized education, training curricula, and career paths that align with both policy objectives and market needs. This challenge underscores the importance of the ECSF. The framework is built upon the European e-Competence Framework (e-CF) to ensure compatibility with existing EU standards. It categorizes cybersecurity skills into technical, behavioral, and transversal competencies, thereby providing a comprehensive and integrated approach (Figure 1).

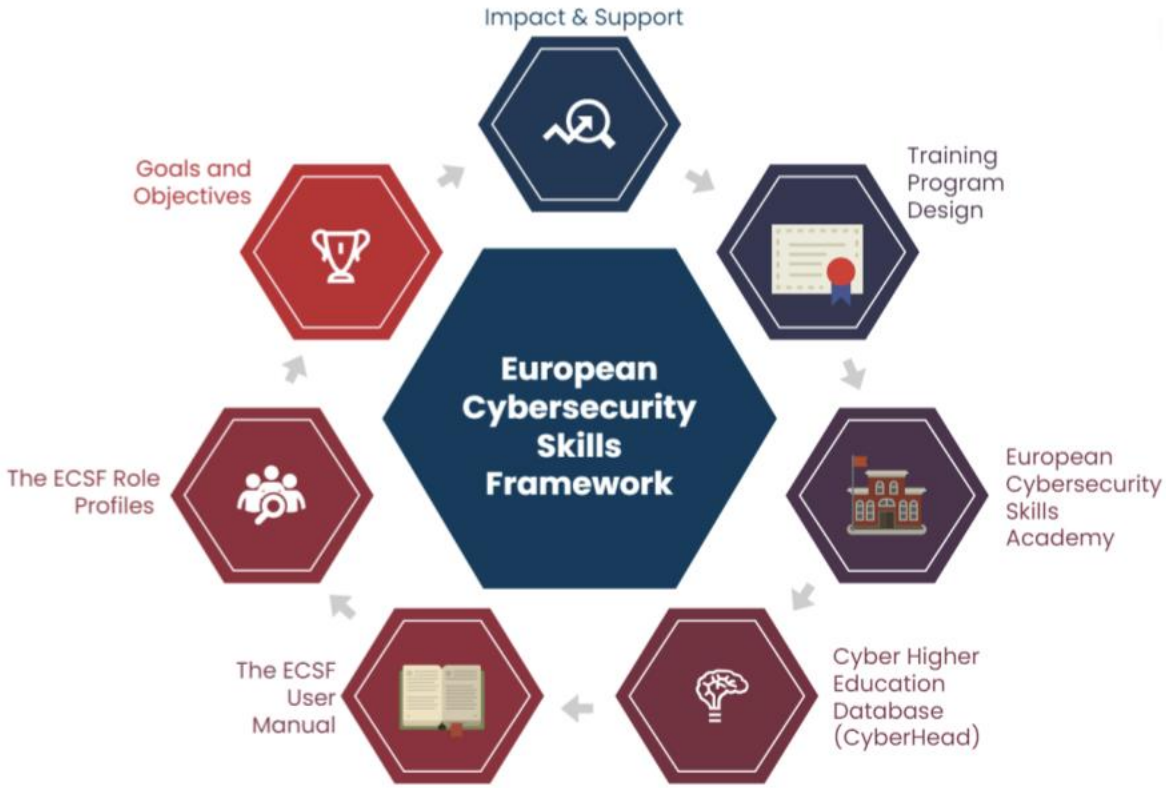

Figure 1: Core features of ECSF

The ECSF comprises twelve (12) role profiles, each tailored to address the cybersecurity workforce demands of European organizations. These profiles are presented in a practical, user-friendly format. Each role profile follows a standardized template that includes the following elements: title, alternative titles, summary statement, mission, main tasks, key skills, key knowledge, and e-Competences. The framework is detailed in two primary documents: the "ECSF Role Profiles" (ENISA, 2022), which outlines the twelve (12) professional role profiles, and the "ECSF User Manual" (ENISA, 2022), which provides targeted guidance on the effective use of the framework.

The twelve role profiles, defined in the ECSF User Manual, are illustrated in the following Figure 2:

Figure 2: The ECSF's 12 Role Profiles for Cybersecurity Professionals

2.1.1 ECSF key principles

The ECSF is founded on a set of principles designed to address stakeholder needs. These guiding principles ensure that the framework is both practical and adaptable, while remaining aligned with European requirements. The principles are as follows:

- **Simple yet Comprehensive:** The framework strives for a balance between simplicity -enabling straightforward adoption- and sufficient detail, thus providing meaningful insights into cybersecurity roles and competencies. This approach ensures broad applicability across organizations of various sizes, sectors, and technical maturity.
- **Flexible and Scalable:** Employing a modular structure, the ECSF's components can be utilized independently or extended as needed. This flexibility facilitates integration with other frameworks, allowing for adaptation to evolving requirements and ongoing updates.
- **Open and Impartial:** Developed through the collaborative efforts of cybersecurity experts from diverse backgrounds, the ECSF incorporates multiple perspectives, thereby reducing bias. As an ENISA publication, it is publicly accessible and intended for widespread utilization.

- **European:** The ECSF aligns with European standards and regulatory frameworks, addressing regional cybersecurity challenges. It complements existing instruments such as the GDPR and emphasizes adherence to ethical and legal standards.

2.1.2 ECSF Guide

The ECSF ensures a common terminology and shared understanding between professional demand and educational supply across the EU. It identifies critical skill requirements, enabling learning providers to develop targeted programs and policymakers to mitigate skill gaps. By clarifying cybersecurity roles, essential skills, and relevant legislation, the ECSF supports HR departments and non-experts in resource planning, recruitment, and career development. It promotes harmonization in education and training, aligning cybersecurity skills with the broader ICT domain. Additionally, the ECSF helps reduce current and future cybersecurity skill shortages while enhancing resilience to cyber-attacks and ensuring secure ICT systems through capacity building within the European workforce.

This guide offers a structured and flexible approach to implementing the European Cybersecurity Skills Framework (ECSF) tailored to various organizational and contextual needs:

1. **Analyse**: Assess the cybersecurity-related conditions of the target environment (e.g., an organization) to establish a baseline. Identify stakeholders and define the objectives
2. **Identify:** Record cybersecurity requirements or goals for the environment. Use the ECSF as a taxonomy to align these objectives with defined roles and competencies
3. **Select**: Choose appropriate ECSF role profiles and components that address the identified needs or achieve the outlined objectives**.**
4. **Adapt**: Customize the chosen ECSF profiles and components to suit the specific context, including mixing, splitting, or tailoring them for sector-specific applications
5. **Apply:** Implement the tailored ECSF components in the target environment to meet cybersecurity objectives and improve overall security posture

2.1.3 ECSF application

2.1.3.1 Apply the ECSF as an Organisation

The ECSF provides a standardized reference for 12 typical cybersecurity roles, enabling organizations to address their specific cybersecurity needs efficiently. The framework offers a structured guide for defining and organizing cybersecurity roles, aligning them with organizational missions, visions, and objectives. It simplifies the process of identifying required roles, managing cybersecurity risks, and structuring cybersecurity departments. Three examples illustrate the practical implementation of the ECSF: (i) enhancing cybersecurity practices in a small company, (ii) supporting recruitment for compliance in a large company, and (iii) planning cybersecurity resources in a large organization.

2.1.3.2 Apply the ECSF as a learning provider

The ECSF establishes a unified language for developing cybersecurity skills, supporting institutions like Higher Education (HE), Vocational Education and Training (VET), and other training programs. The role profiles bridge professional workplace requirements with educational curricula through a European-aligned approach. These

profiles define roles from two perspectives: organizational responsibilities (mission, deliverables, tasks) and learning needs (skills, knowledge, and e-CF competencies).
The ECSF supports academic institutions by many **activities**, i.e., aligning learning outcomes with job market needs, and guiding curriculum design based on role profiles that define relevant skills, knowledge, and competencies. It facilitates collaboration for joint academic programs and student mobility while serving as a foundation for creating standardized cybersecurity curricula and helping universities map and communicate the focus of their programs to students.
The ECSF addresses challenges in the European cybersecurity qualifications landscape by providing standardized terminology for cybersecurity skills across domains and industries. It also supports the development of an integrated platform that offers updated information on the job market, competencies, training courses, certification schemes, and career roadmaps.
The benefits of the ECSF include cross-institution collaboration, learning program mobility, promotion of educational offerings, support for curriculum design, linkage to workplace contexts, assessment of learning programs, and career orientation for students and professionals. Mirroring the approach taken by the NICE framework, the ECSF supports standardized proficiency measures for monitoring student progress, ensuring that educational efforts align closely with evolving industry demands (Wetzel, 2023).

2.1.3.3 Apply the ECSF as an individual professional

The ECSF establishes a common language to align cybersecurity job roles with educational programs, offering clear descriptions of roles, tasks, required skills, competencies, and knowledge. This shared understanding helps attract new individuals to the field and supports career planning in cybersecurity. The ECSF provides a framework for cybersecurity professionals to map their skills and knowledge to desired roles, identify gaps for career progression, and plan transitions between roles. It supports continuous education by facilitating dialogue between employees, while also guiding new entrants through formal and non-formal learning paths.
Cybersecurity offers a viable career opportunity for individuals from other fields, making reskilling an effective way to meet workforce demands and address skill gaps. Due to its multidisciplinary nature, career transitions may be faster for individuals with backgrounds in one of its core areas: technical (technology and solutions to combat cybercrime), human (behavioural aspects, privacy, and awareness), organizational (processes, policies, and inter-organizational cooperation), and regulatory (law, standardization, and forensics)

2.1.3.4 Apply the ECSF as a professional association

The ECSF establishes a common terminology and shared understanding of cybersecurity role profiles, enabling professional associations to standardize their activities across the EU and eliminate confusion in terminology. It supports market analysis to identify high-demand roles, skill gaps, and legislative requirements, while providing professional guidance. The ECSF fosters collaboration among stakeholders, facilitating knowledge sharing, trend identification, peer learning, and multidisciplinary approaches, while empowering customization for specific needs. It serves as a tool for professional associations to enhance cybersecurity resilience across the EU.

2.1.3.5 Apply the ECSF as a policy maker

The ECSF establishes a shared understanding of cybersecurity roles and provides a standardized framework for collecting and sharing workforce-related data and statistics across the EU. This common terminology aids policymakers in gaining insights into the cybersecurity workforce, enabling them to estimate future needs and

maintain the framework's relevance. It facilitates cross-border collaboration, supports market surveys, and enables reliable, comparable data collection on supply and demand for cybersecurity professionals. The ECSF assists policymakers in decision-making related to funding, investments, and intervention periods while aligning EU member states to increase cybersecurity talent and harmonize practices across Europe. In 2023, the Communication on the Cybersecurity Skills Academy and involvement of the European Cybersecurity Competence Centre (ECCC), alongside other initiatives, have further strengthened coordination efforts. These measures aim to enhance alignment between education, certification, and workforce development across EU Member States, thus increasing the ECSF's overall impact.

2.2 ECSO

Cybersecurity is a key priority in the European Commission's policy agenda, as outlined in the EU Security Union Strategy for 2020–2025 (European Comission, 2020). This strategy emphasizes supporting Member States in fostering security. The fourth progress report (May 2022) identifies protecting critical infrastructure, strengthening cyber-resilience, addressing hybrid warfare, and combating disinformation as essential objectives for preparing against emerging challenges. This section provides a detailed overview of the *European Cybersecurity Education & Professional Training: Minimum Reference Curriculum* document (ECSO, 2022), outlining its purpose, structure, and key elements. The document guides to develop essential cybersecurity skills and support sustainable workforce solutions.

2.2.1 Mapping with Best Practices and Frameworks

The report integrates insights from existing best practices, research reports, and frameworks to ensure relevance and applicability:

- **European Commission JRC Technical Report on Proposal for a European Cybersecurity Taxonomy** (European Commission's Joint Research Centre, 2019): aimed to create a comprehensive taxonomy aligning cybersecurity terminologies, definitions, and domains to categorize EU cybersecurity competencies. It incorporates frameworks like the US NICE and IEEE Cybersecurity Curriculum, which are included as part of its recommended best practices.
- **ENISA Reports**: ENISA, established in 2004 and strengthened by the EU Cybersecurity Act, aims to ensure a high level of cybersecurity across Europe. It contributes to EU cyber policy, fosters trust in ICT products through certification and strengthens resilience through collaboration with Member States and stakeholders. This paper incorporates ENISA's prior work, including reports on cybersecurity skills development (ENISA, 2020), privacy and NIS curricula (ENISA, 2015), and education roadmaps (ENISA, 2014).
- **European Cyber Security Body of Knowledge (CyBOK) and IEEE Framework**: The CyBOK project (CyBOK, 2019), originating as a European research initiative, establishes a foundational Cyber Security Body of Knowledge by synthesizing expertise from globally recognized sources. Aligned with IEEE Cybersecurity guidelines, CyBOK provides a structured framework with 19 Knowledge Areas (KAs) to support cybersecurity education at all levels, from secondary to professional development. These KAs inform this paper's curriculum design, ensuring comprehensive coverage of essential cybersecurity domains.

- **ECSO Reports, Practitioners Input and Empirical Market Analysis**: ECSO's Working Group 5 (WG5) focuses on building cybersecurity capacity and capability for a resilient NextGen digital Europe. It emphasizes education, training, skill development, awareness-raising, and gender inclusiveness. WG5's contributions include papers like the Gaps in European Cyber Education and Professional Training (ECSO, 2017), Cybersecurity Awareness Trainings: A Practical Guide (ECSO, 2018), and EHR4CYBER Professional Certification (ECSO, 2020). Leveraging insights from over 270 members and 300 experts, WG5 integrates European perspectives, market needs, and practitioner feedback through reports, workshops, and discussions, supported by the EHR4CYBER network.

2.2.2 Curriculum Development Methodologies and Process

The curriculum development follows a **practitioner-focused analytical and applied science approach**, incorporating desktop research and scientific literature reviews, data collection from experts, and analysis of the information, initial solutions and results, application and developing insights. The process, refined over five years, includes sense-making phases and pilot implementation for practical validation. The minimum reference curriculum adopts a simplified version of **Bloom's taxonomy** (Figure 3) to align with European competency and learning outcome-based pedagogical philosophy. The paper introduces an evidence-based model using a simplified Bloom's taxonomy to structure competence development into three levels: basic, intermediate, and advanced. The curriculum aligns with the European e-Competence Framework (e-CF) to address both knowledge and practical skills. Research highlights the need to revise competency models for greater alignment with real-world cybersecurity practices, ensuring relevance to industry demands. This approach aims to equip professionals with a comprehensive understanding of competencies essential for addressing growing cybersecurity challenges.

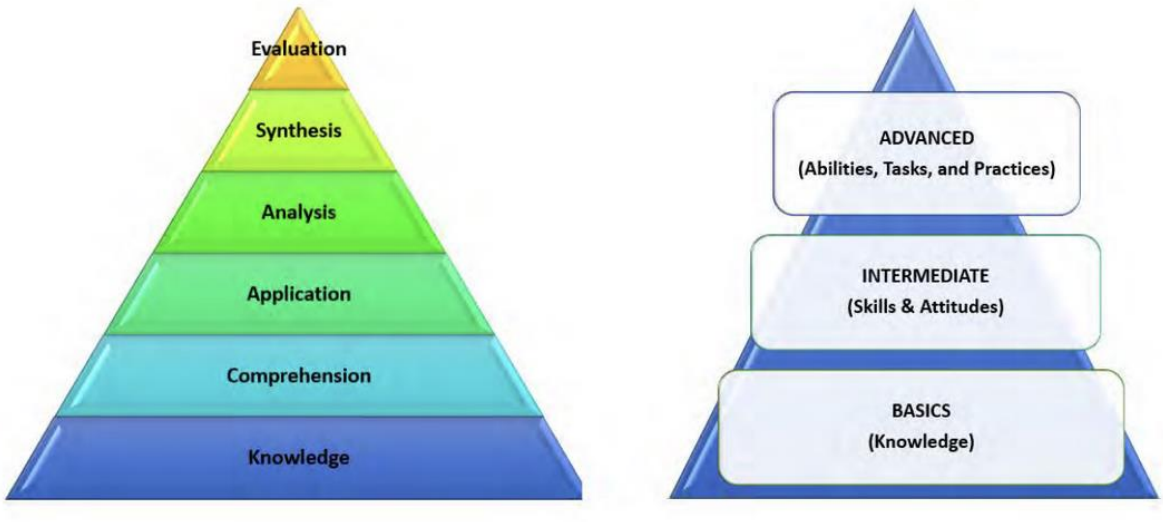

Figure 3: Practitioners' model based upon a simplified Bloom's taxonomy[1]

[1] Scholarly work of the ECSO WG5 Co-chair Paresh Rathod (Laurea-Finland)

The cybersecurity field is rapidly growing, and highly cross-sectoral, demanding candidates possess foundational knowledge, skills, and competencies. ECSO outlines basic, intermediate, and advanced courses to support professional development. Basic courses cover ICT fundamentals, programming, computer architecture, networking, operating systems, and databases, based on the EU DigComp 2.1 framework (European Commission: Joint Research Centre, 2017). Intermediate and advanced courses require these foundational skills as prerequisites, ensuring a structured progression in cybersecurity education. This approach facilitates effective upskilling and prepares candidates for specialized career paths in the cybersecurity domain.

2.2.3 Curriculum Content Structure

The curriculum is organized into four key clusters, each addressing specific aspects of cybersecurity education and training:

Figure 4: High level Curricula Structure and Contents[2]

- **Cybersecurity Principles and Management:** The focus is on foundational knowledge, encompassing risk management, ICT infrastructure security, and regulatory compliance, to equip learners to effectively plan and implement cybersecurity strategies.

[2] Source: Scholarly Work of the ECSO WG5 Co-Chair Paresh Rathod (Laurea-Finland)

- **Cybersecurity Tools and Technologies:** Emphasizes technical skills for managing vulnerabilities, threats, and risks. It provides practical training in using cybersecurity tools and methods through hands-on experiences.
- **Cybersecurity in Modern and Emerging Digital Technologies:** Covers cutting-edge areas like AI, IoT, and blockchain, aiming to prepare learners to address security challenges in modern and future digital environments.
- **Cybersecurity Practitioners and Technical Security Validation:** Focuses on advanced topics such as threat analysis. It trains learners in offensive security techniques and technical security validation.

2.2.4 Reference Curriculum

The curriculum provides a detailed template for each module, including subject codes, competence levels, and learning outcomes. The modules cover a range of topics including ICT infrastructure and security, cybersecurity principles, information and cybersecurity management, project management, enterprise cybersecurity practice, network and application security, vulnerability assessment, cybersecurity for AI, machine learning security, cloud technologies, digital transformation, ethical hacking, cyber ranges, digital forensics and IoT cybersecurity, providing a comprehensive approach to developing skills and competencies in the cybersecurity field.

2.2.5 Key Takeaways

The analysis of these frameworks provided valuable insights into the roles and competencies expected of cybersecurity professionals, while also revealing gaps in existing training approaches. Specifically:

1. **Defining Roles and Competencies**: The frameworks helped delineate the core responsibilities and skill sets required for various cybersecurity roles, which in turn informed the design of our training modules.
2. **Identifying Training Gaps**: Recurring gaps were identified in current curricula, including insufficient emphasis on hands-on problem-solving, real-world scenarios, and coverage of emerging threats.
3. **Curriculum Structuring**: Guided by the frameworks, we developed a comprehensive and modular training curriculum aligned with industry expectations and professional standards.

Building on these findings, our project develops a training platform that embeds these insights into its foundational design. It features role-specific learning paths, addresses skill gaps with targeted content, and employs scenario-based learning to bolster practical expertise. This alignment ensures the platform remains both relevant and impactful for cybersecurity professionals at different career stages.

The review of modules in this deliverable underscores the importance of cyber ranges as a standard hands-on learning method within the Minimum Reference Curriculum. While simulation labs are commonly utilized, they often lack sustainability and accessibility unless integrated with cyber ranges-especially given challenges such as restricted campus access during COVID-19. ECSO WG5 advocates for broader adoption of cyber range-based services to democratize advanced educational tools, thereby complementing traditional methods like instructor-led education, self-directed learning, and ongoing professional development. ECSO also plans to update this report to reflect the perspectives of the wider cybersecurity community and to incorporate additional frameworks like the European Cybersecurity Skills Framework.

3 Proposed skills development approach

Cybersecurity skills development training program lifecycle

Cybersecurity skills development training programs must be proactively managed throughout their entire lifecycle, requiring continuous attention and adjustments. Managers of those programs should meticulously outline, discuss, review, and document the program's objectives and available options. By adopting effective strategies and developing comprehensive planning approaches that include regular measurement and feedback, an organization ensures that the training programs' objectives remain aligned with their overall goals. Figure 5 highlights the key phases of developing and managing a learning program: Planning and Strategy, Analysis and Design, Development and Implementation, and Assessment and Improvement. These phases can be carried out sequentially or concurrently. At any point in the lifecycle, cybersecurity skills development training programs' managers and their teams may engage in activities such as curriculum development, evaluating instructor feedback, distributing practical exercise email quizzes, designing awareness posters, or creating presentations for senior leadership.

Figure 5: Cybersecurity and Privacy Learning programs' lifecycle (Merritt, et al., 2024)

Broadly speaking, cybersecurity skills development training programs are essential components of the organization's learning culture. To be effective, the training programs must be aligned with organizational goals and considered adaptive, continuous, and evolving. In a learning organization, employees can expand and enhance their existing capabilities to understand and meet new mission requirements. Employees are valued for their ability to create and inspire others and are actively involved in achieving lifelong learning accomplishments. When an organization offers additional learning programs (e.g., career development, leadership, and executive development), training programs should be similarly integrated into the organization-wide learning framework.

3.1 NG-SOC skills development training program strategy (Plan & Strategy phase)

This section outlines the process through which the proposed skills development strategy report was formulated, drawing on the training requirements provided by the NG-SOC pilot partners (CXB, CYNET, ELES, INFORMATICA). To ensure that all partners were familiarized with the fundamental principles of the ECSF, UPRC initially organized four (4) dedicated workshops.

- On 15/3/2024 with Informatica,
- On 26/3/2024 with CYNET,
- On 28/3/2024 with ELES and
- On 4/4/2024 with CXB

Subsequently, and in alignment with the ECSF, UPRC requested that the participating partners specify their training needs for the cybersecurity awareness program. This involved identifying which organizational role profiles required reskilling or upskilling.

With respect to the tasks, knowledge, skills, and competencies associated with each ECSF security role profile, the NG-SOC pilots were provided with the ECSF spreadsheet (available at the ENISA website: https://www.enisa.europa.eu/sites/default/files/2024-12/ECSF.xlsx). Each pilot was asked to review and mark the specific requirements most relevant to their organization's needs:

- with red color the row(s) (per knowledge/skill/e-competence) where there was a complete lack/gap of a certain knowledge/skill/competence,
- with blue color the row(s) (per knowledge/skill/e-competence) where there was a complete lack/gap of a certain knowledge/skill/competence and thus upskilling (i.e., acquire new knowledge/skill/e-competence from scratch) was required, and
- with orange color the row(s) (per knowledge/skill/e-competence) where there was a need for reskilling (i.e., someone already possesses a certain level of knowledge/skill/competence but may benefit from training intervention for improvement or acquire skills that were directly relevant within one's current profession).

	Chief Information Security Officer (CISO)	Cyber Incident Responder	Cyber Legal, Policy & Compliance Officer	Cyber Threat Intelligence Specialist	Cybersecurity Architect	Cybersecurity Auditor	Cybersecurity Educator	Cybersecurity Implementer	Cybersecurity Researcher	Cybersecurity Risk Manager	Digital Forensics Investigator	Penetration Tester
Knowledge Blue	13	14	19	18		15				14	14	8
Knowledge Orange	1	2	3	1	5	3	1	3	1	6		
Knowledge Red	0							1				1
TOTAL	14	16	22	19	5	18	1	4	1	20	14	12
	Chief Information Security Officer (CISO)	Cyber Incident Responder	Cyber Legal, Policy & Compliance Officer	Cyber Threat Intelligence Specialist	Cybersecurity Architect	Cybersecurity Auditor	Cybersecurity Educator	Cybersecurity Implementer	Cybersecurity Researcher	Cybersecurity Risk Manager	Digital Forensics Investigator	Penetration Tester
Skills Blue	22	13	30	8		29				32	14	8
Skills Orange	6		4	6				2		2		
Skills Red	1			3				1				
TOTAL	29	13	34	17	0	29	0	3	0	34	14	8
OVERALL	43	29	56	36	5	47	1	7	1	54	28	20
	Rewire	Rewire		Rewire								Rewire

Figure 6: Identified training needs per ECSF role

Through comprehensive analysis of the collected responses, a matrix was generated/created (Figure 6) where it was identified that four (4) roles -Architect, Educator, Implementer, and Researcher- demonstrated minimal interest in terms of the required knowledge and skills for the cybersecurity training program.

Besides that, the analysis of the use-cases developed by the pilots (for the sake of Task 2.1 of the NG-SOC) revealed that, although the initial general requirements elicitation phase encompassed most of the ECSF roles, only a subset of them was present in the specific NG-SOC use-case scenarios (Figure 7). Specifically, the roles that appeared most frequently in the use-case scenarios were the Incident Responder, the CTI, the Auditor, the Educator, the Implementer, the Risk Manager, and the Pentester. However, training material for four roles (namely the CISO, the Incident Responder, the CTI, and the Pentester) is already provided by the REWIRE learning

platform (https://vle.rewireproject.eu/). A member of the NG-SOC consortium, Caixa Bank (CXB), also participated in the REWIRE project and contributed significantly to the development of its learning platform and training material. Since the REWIRE training material are openly accessible, they can be utilized within the NG-SOC project if necessary. As a result, developing similar training material for the four ECSF roles hosted on the REWIRE learning platform was deemed unnecessary. Instead, the NG-SOC training initiative will focus exclusively on the four ECSF roles identified as critical to this project: CPO, Auditor, Risk Manager, and Digital Forensics Investigator. For the roles covered in REWIRE, the existing materials will be evaluated and, where necessary, augmented with additional modules to meet the specific requirements of the NG-SOC training program.

-----	ECSF ROLE PROFILES																							
	1		2		3		4		5		6		7		8		9		10		11		12	
PARTNERS	CISO		Incident Responder (SOC Analyst)		CPO		CTI		Architect		Auditor		Educator		Implementer		Researcher		Risk Manager		Digital Forensics Investigator		Pentester	
	Requirement	Use-Cases	Requirement	Use-Cases	Requirement	Use-Cases	Requirement	Use-Cases	Requirement	Use-Cases	Requirement	Use-Cases	Requirement	Use-Cases	Requirement	Use-Cases	Requirement	Use-Cases	Requirement	Use-Cases	Requirement	Use-Cases	Requirement	Use-Cases
CXB	✔	✗	✔	✔	✔	✗	✔	✔	✗	✗	✔	✔	✗	✔	✗	✗	✗	✗	✔	✔	✔	✔	✔	✔
CYNET	✔	✗	✔	✔	✔	✗	✔	✔	✔	✗	✔	✔	✔	✔	✔	✔	✔	✗	✔	✔	✗	✗	✗	✔
ELES/INFO	✗	✔	✔	✔	✗	✗	✔	✔	✗	✗	✗	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔	✗	✗	✗

Figure 7: Combined training requirements derived from identified training needs per ECSF role and ECSF roles engaged in the NG-SOC use-case scenarios

Considering all the above, a modular approach was proposed for the NG-SOC skills development program. In the modular approach, the distinct knowledge, skills, and e-Competences requirements that were derived from the ECSF framework and elicitated by the NG-SOC partners based on their training needs, were grouped based on their resemblance. For each specific group, a learning module was formed. In this way, learning modules can be combined in any way required for covering the needs of an ECSF role profile.

Building upon the insights derived from the frameworks presented in the previous section, we leveraged their role definitions, skill benchmarks, and identified gaps to shape the foundational structure of our training development process. These frameworks provided a standardized reference for aligning the competencies targeted in our training modules with industry-recognized expectations, ensuring relevance and applicability. The learning modules that were developed based on the bottom-up approach are the following:

Learning Module 0: Introductory section

Entails basic terminology and core knowledge in cybersecurity for attendees that completely lack knowledge and skills in this field.

Learning Module 1: Cybersecurity Laws, Regulations, and Compliance

- Skills:
  - Analyze and comply with cybersecurity-related laws and regulations.
  - Explain and communicate data protection and privacy topics to stakeholders.
  - Adapt legal and regulatory requirements to business needs.
  - Understand implications of legal framework modifications on cybersecurity policies.
- Knowledge:
  - Cybersecurity-related laws, regulations, and legislations.
  - Cross-domain knowledge related to cybersecurity.
- e-Competences:
  - E.9. Information Systems Governance.

Learning Module 2: Risk Management and Compliance

- Skills:
  - Analyse and consolidate organisation's quality and risk management practices
  - Define and apply maturity models for cybersecurity management
  - Develop, champion and lead the execution of a cybersecurity strategy
  - Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks
  - Propose and manage risk-sharing options
- Knowledge:
  - Risk management recommendations and best practices
  - Risk management standards, methodologies and frameworks
  - Cybersecurity risks
- e-Competences:
  - E.3. Risk Management
  - E.8. Information Security Management
  - E.6. ICT Quality Management

Learning Module 3: Auditing and Assessment

- Skills:
  - Apply auditing tools and techniques
  - Audit with integrity, being impartial and independent
  - Collect, evaluate, maintain and protect auditing information
  - Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools
  - Follow and practice auditing frameworks, standards and methodologies
- Knowledge:
  - Auditing standards, methodologies and frameworks
  - Auditing-related certifications

Learning Module 4: Cybersecurity Policies and Frameworks

- Skills:
  - Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks
  - Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties
  - Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards
  - Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing
  - Review and enhance security documents, reports, SLAs and ensure the security objectives
- Knowledge:
  - Cybersecurity standards, methodologies and frameworks
  - Conformity assessment standards, methodologies and frameworks
  - Cybersecurity-related certifications
- e-Competences:
  - E.8. Information Security Management

- E.5. Process Improvement
- E.6. ICT Quality Management

Learning Module 5: Technical Analysis and Security Management

- Skills:
  - Assess and enhance an organisation's cybersecurity posture
  - Conduct technical analysis and reporting
  - Decompose and analyse systems to identify weaknesses and ineffective controls
  - Identify threat actors TTPs and campaigns
  - Manage and analyse log files
  - Manage cybersecurity resources
  - Work on operating systems, servers, clouds and relevant infrastructures
  - Propose and manage risk-sharing options
  - Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks
  - Implement cybersecurity recommendations and best practices

- Knowledge:
  - Computer networks security
  - Computer programming
  - Computer systems vulnerabilities
  - Malware analysis tools
  - Secure coding recommendations and best practices
  - Security architecture reference models
  - Risk management tools
  - Risk management recommendations and best practices
- e-Competences:
  - B.2. Component Integration
  - B.3. Testing
  - C.4. Problem Management
  - D.7. Data Science and Analytics
  - B.5. Documentation Production

Learning Module 6: Business Integration and Strategy

- Skills:
  - Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls
  - Communicate, present and report to relevant stakeholders
  - Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements
  - Establish a cybersecurity plan
  - Influence an organisation's cybersecurity culture
  - Motivate and encourage people
- Knowledge:
  - Cybersecurity awareness, education and training programme development
  - Cybersecurity trends
  - Multidiscipline aspect of cybersecurity

- e-Competences:
  - A.1. Information Systems and Business Strategy Alignment
  - A.7. Technology Trend Monitoring
  - E.7. Business Change Management

Learning Module 7: Privacy and Data Protection

- Skills:
  - Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy
  - Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools
  - Explain and communicate data protection and privacy topics to stakeholders and users
- Knowledge:
  - Privacy-Enhancing Technologies (PET)
  - Digital forensics recommendations and best practices
- e-Competences:
  - D.10. Information and Knowledge Management

Learning Module 8: Incident Response and Forensics

- Skills:
  - Identify and solve cybersecurity-related issues
  - Identify non-cyber events with implications on cyber-related activities
  - Work under pressure
  - Conduct technical analysis and reporting
- Knowledge:
  - Incident handling recommendations and best practices
  - Incident handling standards, methodologies and frameworks
  - Computer Security Incident Response Teams (CSIRTs) operation
  - Criminal investigation procedures, standards, methodologies and frameworks
  - Digital forensics recommendations and best practice

Learning Module 9: Collaboration and Communication

- Skills:
  - Collaborate with other team members and colleagues
  - Communicate, coordinate and cooperate with internal and external stakeholders
  - Organise and work in a systematic and deterministic way based on evidence
- Knowledge:
  - Cybersecurity awareness, education and training programme development
  - Multidisciplinary aspect of cybersecurity

3.2 Analysis & Design phase: OpenEdX Learning Platform overview

3.2.1 Introduction

OpenEdX is a versatile and highly customizable open-source learning management system (LMS) distinguished by its modularity, scalability, and open architecture. Unlike many proprietary LMS platforms, OpenEdX enables

institutions to tailor every aspect of the platform-from content presentation to integrations-to suit unique pedagogical and operational requirements. Its robust support for multilingual and diverse learning environments further sets it apart, making it a preferred choice for global education initiatives. It provides institutions, corporations, and non-profits with scalable and multilingual solutions, enabling global reach and diverse learner engagement. Serving as the foundation for edX.org, OpenEdX powers over 3,000 courses and supports millions of learners worldwide. Within the NG-SOC initiative, OpenEdX will play a central role in curating and delivering skill-building resources that align with the project's educational objectives.

3.2.2 Core Functions of OpenEdX

OpenEdX offers an extensive range of functionalities tailored for modern educational environments, including content delivery, course management, assessment tools, and collaborative features.

a. **Content Delivery**: The platform supports diverse content formats such as interactive videos, multimedia presentations, text-based resources, and integrated assessments. For example, interactive videos can be used to simulate real-world scenarios in technical training, allowing learners to engage with branching scenarios and make decisions in a controlled environment. Multimedia presentations have been employed in corporate onboarding to deliver visually rich, step-by-step tutorials on company processes. Text-based resources, such as case studies and articles, are often integrated into professional development programs to foster critical analysis. Additionally, integrated assessments like quizzes and peer-reviewed assignments are frequently used in online certification programs to validate knowledge and skills effectively. Third-party integrations allow for additional specialized content, ensuring flexibility and engagement for learners.
b. **Course Management**: OpenEdX provides modular course structuring, an intuitive content-authoring tool called Studio, and branding customization to align with institutional identity. These features enable educators to design courses tailored to specific pedagogical objectives while maintaining professionalism.
c. **Assessment and Feedback**: To facilitate effective learning, OpenEdX incorporates tools such as automated quizzes, peer assessments, and progress tracking. These features support both formative and summative evaluations, ensuring a comprehensive assessment experience.
d. **Collaboration**: Collaborative tools, including discussion forums, synchronous learning integrations (e.g., Zoom, Microsoft Teams), and internal messaging systems, enhance interactivity and create dynamic learning environments.

3.2.3 Advanced Capabilities

Expanding beyond its foundational features, OpenEdX integrates a suite of advanced capabilities that enhance scalability, foster inclusivity, and support data-driven decision-making:

a. **Scalability and Integration**: OpenEdX excels in scalability, supporting large-scale educational initiatives without compromising performance. Its ability to integrate with analytics platforms, gamification tools, and external content repositories extends its functionality, enriching learner engagement and streamlining administrative processes.
b. **Accessibility and Inclusivity**: Adhering to Web Content Accessibility Guidelines (WCAG), OpenEdX ensures accessibility for learners with disabilities by incorporating features such as keyboard navigation, screen reader compatibility, and customizable display settings. These tools help to remove barriers to access, enabling a more inclusive learning environment for users with visual, auditory, motor, or

cognitive impairments. Its multilingual capabilities make it ideal for diverse cultural and linguistic contexts, further expanding its applicability.

c. **Data-Driven Insights**: The platform provides robust analytics and reporting tools, enabling educators and administrators to gain actionable insights into learner behaviour and performance. These tools support data-driven decision-making for continuous improvement.

3.2.4 Role in NG-SOC Project

Within the NG-SOC project, OpenEdX serves as a foundational tool in the Analysis & Design phase of instructional development. Its modular architecture and feature-rich environment enable the delivery of tailored educational content designed to address specific skill development goals.

a. **Tailored Educational Resources**: The platform will host interactive modules, collaborative projects, and structured assessments to facilitate practical skill acquisition. Its analytics tools allow for iterative refinement of content and teaching strategies, ensuring alignment with learner needs.
b. **Enhanced Collaboration**: Collaborative features, including forums and live communication tools, will foster peer-to-peer learning and instructor-led interactions. This ecosystem supports knowledge sharing and collective problem-solving.
c. **Comprehensive Tracking**: OpenEdX's tracking and reporting capabilities provide transparent insights into learner progression. This supports stakeholders in making informed decisions and aligning instructional strategies with project objectives.
d. **Potential for Future Expansion**: As an open-source platform, OpenEdX is equipped for continuous evolution. Organizations can develop custom plugins or integrate emerging technologies to expand its capabilities. AI-driven analytics can personalize learning paths by analyzing learner interactions to recommend targeted content, such as supplementary modules for struggling learners or advanced materials for high performers.

3.3 Analysis & Design phase: KYPO Cyber Range Platform for Realistic Cybersecurity Training

The KYPO Cyber Range Platform is a key component of the NG-SOC project, designed to bridge the gap between theoretical knowledge and practical application. By providing a scalable and immersive environment for training, KYPO enables participants to simulate and respond to realistic cyber threats in controlled scenarios, ensuring their preparedness for modern cybersecurity challenges.

3.3.1 Key Benefits and Features

The KYPO platform offers several unique capabilities that make it an essential tool for developing realistic cybersecurity training and exercise scenarios:

- **Flexible Design**: KYPO allows for modular and adaptable training configurations tailored to the specific needs of diverse organizations and ECSF-aligned role profiles.
- **Scalable Architecture**: The platform supports large-scale training programs, accommodating multiple participants simultaneously without compromising performance.

- **Immersive Realism**: Participants engage with simulations that replicate real-world cyber threats, enhancing their ability to identify vulnerabilities, respond to incidents, and manage crises effectively.

3.3.2 Role in the NG-SOC Project

Within the NG-SOC initiative, the KYPO Cyber Range complements the broader goals of hands-on, scenario-based learning by:

- **Enhancing Practical Skills**: Trainees develop and refine their skills in areas such as incident response, threat analysis, and digital forensics through interactive exercises.
- **Aligning with Industry Standards**: The scenarios are designed to reflect current industry practices and technological advancements, ensuring relevance to real-world cybersecurity needs.
- **Fostering Collaboration**: KYPO enables teamwork by supporting collaborative training sessions where participants solve complex problems in simulated environments.

3.3.3 Integration and Future Potential

The KYPO platform works in tandem with other NG-SOC tools, such as the OpenEdX platform, to create a comprehensive cybersecurity training ecosystem. This integration ensures that trainees benefit from both theoretical learning and practical application. Furthermore, KYPO's modularity allows for future enhancements, such as the inclusion of advanced AI-driven analytics to personalize training scenarios and track participant progress.

By embedding KYPO into the NG-SOC training framework, the project ensures that learners are equipped with the skills necessary to address evolving cybersecurity challenges, making them valuable assets in safeguarding digital infrastructure.

4 Alignment of proposed training syllabus with the ECSO template

In this section, the proposed syllabus for the NG-SOC project is incorporated to the ECSO template which demonstrates that the recommended skills development strategy is fully aligned with the ECSO minimum curriculum requirements.

Table 1: Module 1: Cybersecurity Laws, Regulations, and Compliance

<table>
<tr><th colspan="2">Competence Level: Basic / Intermediate</th></tr>
<tr><td colspan="2">This module introduces the legal and regulatory frameworks governing cybersecurity, including international and EU-specific regulations. It examines ethical considerations, especially in emerging areas like AI, and provides an overview of governance and compliance standards. Through case studies, learners will understand the practical application of these laws, their ethical implications, and how to maintain compliant information systems.</td></tr>
<tr><th>Subject contents and topics</th><th>Learning outcomes (competences)</th></tr>
<tr><td rowspan="3">> Introduction to Cybersecurity
> Cybersecurity Laws and Regulations, Legal and Ethical issues in the Artificial Intelligence era
> Ethical Considerations in Cybersecurity Information Systems Governance
> Case Studies and Practical Applications Review and Assessment</td><td>The student is able to:
- Understand foundational cybersecurity laws and regulations at global and EU levels.
- Identify key legal and ethical issues in cybersecurity, including those arising from AI technologies.
- Apply principles of governance and compliance in information security management.
- Evaluate case studies to understand the real-world implications of legal and ethical standards.
- Develop a baseline ability to incorporate compliance measures into organizational cybersecurity practices.</td></tr>
<tr><th>Mapping with ENISA ECSF</th></tr>
<tr><td>Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager, Cybersecurity Auditor.</td></tr>
</table>

Table 2: Module 2: Risk Management

<table>
<tr><td colspan="2">Competence Level: Intermediate / Advanced</td></tr>
<tr><td colspan="2">This module focuses on the principles and practices of cybersecurity risk management. It covers fundamental concepts of identifying and assessing risks, understanding risk appetite, and implementing effective risk treatment strategies. Students will learn to propose and manage mitigation options, select and apply relevant information security controls, and leverage maturity models to enhance cybersecurity management. Through practical exercises and case studies, learners will gain hands-on experience in evaluating and improving risk management frameworks.</td></tr>
<tr><td>Subject contents and topics</td><td>Learning outcomes (competences)</td></tr>
<tr><td rowspan="2">> Introduction to Risk Management
> Risk Apetite, Risk Assessment, and Risk Treatment
> Proposing and Managing Risk Mitigations Strategy and Options
> Information Security Controls
> Maturity Models for Cybersecurity Management
> Practical Exercises and Case Studies
> Review and Assessment</td><td>The student is able to
- Identify and categorize cybersecurity risks and their potential impacts on organizational assets.
- Assess risk appetite, conduct risk assessments, and develop risk treatment plans aligned with business objectives.
- Propose effective mitigation strategies and select appropriate security controls to reduce identified risks.
- Apply maturity models to evaluate and enhance the organization’s cybersecurity posture.
- Analyze case studies to refine practical risk management decision-making skills.</td></tr>
<tr><td>Mapping with ENISA ECSF
Cybersecurity Risk Manager, Cybersecurity Auditor.</td></tr>
</table>

Table 3: Module 3: Auditing and Assessment

<table>
<tr><th colspan="2">Competence Level: Intermediate / Advanced</th></tr>
<tr><td colspan="2">This module provides a comprehensive understanding of cybersecurity auditing and assessment processes. It begins with fundamental auditing concepts and the evaluation of auditor competence, then explores recognized standards, frameworks, and methodologies. Learners will gain knowledge on managing audit programs, conducting thorough audits, performing data protection and privacy impact assessments, and working toward relevant certifications. Practical exercises and case studies will help translate theoretical knowledge into applied auditing skills.</td></tr>
<tr><th>Subject contents and topics</th><th>Learning outcomes (competences)</th></tr>
<tr><td rowspan="2">> Introduction to Auditing

> Principles of Auditing, Competence and Evaluation of Auditors

> Auditing Standards, Methodologies, Frameworks, and Tools

> Managing an Audit Programme

> Conducting an Audit

> Conducting Data Protection Impact Assessments / Privacy Impact Assessments

> Auditing-Related Certification

> Practical Exercises and Case Studies

> Assessment</td><td>The student is able to

- Understand fundamental principles and standards of cybersecurity auditing.

- Evaluate auditor competence and apply recognized methodologies, frameworks, and tools.

- Manage an audit program, from planning and resource allocation to reporting findings.

- Conduct data protection and privacy impact assessments to ensure compliance and safeguard personal information.

- Prepare for audit-related certifications to enhance professional credibility.</td></tr>
<tr><td>Mapping with ENISA ECSF

Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager, Cybersecurity Auditor.</td></tr>
</table>

Table 4: Module 4: Cybersecurity Policies and Frameworks

<table>
<tr><th colspan="2">Competence Level: Intermediate / Advanced</th></tr>
<tr><td colspan="2">This module focuses on the creation, implementation, and maintenance of effective cybersecurity policies and frameworks. It covers international and industry standards, supply chain security policies, and the application of Information Security Management Systems (ISMS). Learners will explore strategies for process improvement and quality management, ensuring that cybersecurity measures align with organizational objectives and compliance requirements.</td></tr>
<tr><th>Subject contents and topics</th><th>Learning outcomes (competences)</th></tr>
<tr><td rowspan="2">> Understanding and Developing Cybersecurity Policies and Frameworks
> Cybersecurity standards
> Cybersecurity Policies in the Supply chain
> Information Security Management Systems (ISMS)
> Process Improvement and Quality Management
> Review and Assessment</td><td>The student is able to
- Understand key cybersecurity standards and frameworks (e.g., ISO/IEC 27001).
- Develop and implement tailored cybersecurity policies, including those governing supply chain activities.
- Establish and maintain an effective ISMS aligned with organizational goals and regulatory requirements.
- Apply principles of process improvement and quality management to enhance the cybersecurity posture.
- Critically review and assess existing policies to ensure their relevance, effectiveness, and continuous improvement.</td></tr>
<tr><td>Mapping with ENISA ECSF
Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager, Cybersecurity Auditor, Cybersecurity Implementer.</td></tr>
</table>

Table 5: Module 5: Technical Analysis and Security Management

Competence Level: Intermediate / Advanced	
This module delves into the technical aspects of cybersecurity, covering a broad range of topics including network and system security, secure programming, malware analysis, vulnerability management, and security architecture. Learners will gain hands-on experience with tools and techniques for analyzing threats, implementing secure software development practices, managing logs, and configuring secure infrastructures (including cloud environments). Through practical exercises and case studies, they will learn to identify threat actors, apply security best practices, and assess the effectiveness of cybersecurity controls.	
Subject contents and topics	**Learning outcomes (competences)**
> Introduction to Technical Analysis and Security Management > Computer and Communication Network Security > Computer Programming for Security Professionals > Computer Systems Vulnerabilities > Malware Analysis Tools > Secure Software Development and Best Practices > Security Architecture Reference Models Identifying Threat Actors, Vulnerabilities management and TTPs > Log File Management and Analysis > Working with Operating Systems, Servers, and Cloud Infrastructures > Implementing Cybersecurity Recommendations and Best Practices > Assessing Cybersecurity Controls > Practical Exercises and Case Studies > Assessment	The student is able to - Understand fundamental and advanced principles of computer and communication network security. - Apply secure programming and software development best practices to mitigate vulnerabilities. - Identify and analyze computer system vulnerabilities, malware, threat actors, and their Tactics, Techniques, and Procedures (TTPs). - Implement security architecture models and deploy effective security controls across operating systems, servers, and cloud infrastructures. - Use log management and analysis techniques to detect, respond to, and prevent security incidents. - Assess and validate cybersecurity controls to ensure robust protection and compliance with best practices.
	Mapping with ENISA ECSF
	Cybersecurity Implementer, Digital Forensics Investigator, Cyber Incident Responder, Cybersecurity Architect.

Table 6: Module 6: Business Integration and Strategy

<table>
<tr><th colspan="2">Competence Level: Intermediate / Advanced</th></tr>
<tr><td colspan="2">This module bridges the gap between cybersecurity and organizational objectives. It guides learners on how to align cybersecurity strategies with broader business goals, analyze processes to identify and implement appropriate security controls, and stay abreast of evolving technological and cybersecurity trends. Additionally, it covers effective communication with stakeholders, methods to influence cybersecurity culture, and approaches to integrating cybersecurity awareness and privacy considerations into business decision-making.</td></tr>
<tr><th>Subject contents and topics</th><th>Learning outcomes (competences)</th></tr>
<tr><td>> Introduction to Cybersecurity
> Cybersecurity Laws and Regulations, Legal and Ethical issues in the Artificial Intelligence era
> Ethical Considerations in Cybersecurity
Information Systems Governance
> Case Studies and Practical Applications
Review and Assessment
> Aligning Cybersecurity with Business Strategy
> Analyzing Business Processes and Security Controls
> Technology Trend Monitoring and Cybersecurity Trends
> Establishing a Cybersecurity Plan
> Communication and Stakeholder Engagement
> Cybersecurity and Privacy Awareness, Influencing Cybersecurity Culture and Managing Change
> Review and Assessment</td><td>The student is able to
- Align cybersecurity strategies, plans, and controls with organizational business objectives.
- Evaluate and integrate cybersecurity considerations into business processes and workflows.
- Monitor emerging technology and cybersecurity trends to inform strategic decision-making.
- Develop and maintain a comprehensive cybersecurity plan that includes communication strategies and stakeholder engagement.
- Foster a strong cybersecurity culture within the organization, influencing behaviour and managing change effectively.

Mapping with ENISA ECSF
Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager, Cybersecurity Architect.</td></tr>
</table>

Table 7: Module 7: Privacy and Data Protection

<table>
<tr><th colspan="2">Competence Level: Intermediate / Advanced</th></tr>
<tr><td colspan="2">This module provides a comprehensive understanding of privacy and data protection principles, focusing on the legal, ethical, and regulatory frameworks that govern personal data in the digital era. It addresses challenges introduced by Artificial Intelligence (AI), emphasizes conducting Data Protection Impact Assessments (DPIAs) and Privacy Impact Assessments (PIAs), and explores the use of Privacy-Enhancing Technologies (PET). Learners will also understand how privacy considerations intersect with digital forensics, ensuring data protection obligations are met throughout the investigative process.</td></tr>
<tr><th>Subject contents and topics</th><th>Learning outcomes (competences)</th></tr>
<tr><td rowspan="2">> Introduction to Privacy and Data Protection

> Privacy and Data Protection Legal and Ethical issues in the Artificial Intelligence era

> Conducting Data Protection Impact Assessments / Privacy Impact Assessments

> Implementing Privacy-Enhancing Technologies (PET)

> Privacy-preservation and Digital Forensics

> Review and Assessment</td><td>The student is able to

- Understand global and EU data protection laws, regulations, and ethical considerations, including those related to AI.

- Conduct DPIAs/PIAs to identify, evaluate, and mitigate privacy risks.

- Apply Privacy-Enhancing Technologies (PET) to protect personal data throughout its lifecycle.

- Integrate privacy considerations into digital forensic procedures, ensuring evidence handling does not infringe on individual rights.

- Embed privacy and data protection best practices into organizational policies, ensuring compliance and trustworthiness.</td></tr>
<tr><td>Mapping with ENISA ECSF

Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager.</td></tr>
</table>

Table 8: Module 8: Incident Response and Forensics

Competence Level: Intermediate / Advanced	
This module focuses on the skills and knowledge needed to effectively prepare for, detect, respond to, and recover from cybersecurity incidents. It covers established incident handling standards, methodologies, and frameworks, as well as the roles and operations of Computer Security Incident Response Teams (CSIRTs). Learners will gain experience in conducting technical analysis, documenting findings, and working within criminal investigation procedures, while adhering to digital forensics best practices. Through practical exercises and case studies, participants will develop the competencies necessary to manage incidents and support forensic investigations.	
Subject contents and topics	**Learning outcomes (competences)**
> Introduction to Cybersecurity > Cybersecurity Laws and Regulations, Legal and Ethical issues in the Artificial Intelligence era > Ethical Considerations in Cybersecurity Information Systems Governance > Case Studies and Practical Applications Review and Assessment > Introduction to Incident Response and Forensics > Identifying Cybersecurity-Related Issues > Incident Handling Standards, Methodologies, and Frameworks > Operation of Computer Security Incident Response Teams (CSIRTs) > Conducting Technical Analysis and Reporting > Criminal Investigation Procedures in Cybersecurity > Digital Forensics Best Practices > Practical Exercises and Case Studies > Assessment	The student is able to: - Understand the incident response lifecycle, including preparation, detection, analysis, containment, eradication, and recovery. - Apply recognized standards, methodologies, and frameworks to structure and guide incident handling efforts. - Operate effectively as part of or in collaboration with CSIRTs, coordinating tasks and sharing critical information. - Conduct technical analyses to identify root causes, impacted systems, and nature of incidents, ensuring proper documentation and reporting. - Follow criminal investigation procedures and digital forensics best practices to preserve evidence integrity and support potential legal actions. **Mapping with ENISA ECSF** Cyber Threat Intelligence Specialist, Cyber Incident Responder, Digital Forensics Investigator, Cyber Legal, Policy & Compliance Officer.

Table 9: Module 9: Collaboration and Communication

<table>
<tr><th colspan="2">Competence Level: Basic / Intermediate</th></tr>
<tr><td colspan="2">This module emphasizes the importance of effective communication, teamwork, and interdisciplinary collaboration in cybersecurity contexts. It covers strategies for clear stakeholder communication, evidence-based decision-making, and the development of cybersecurity awareness programs. By integrating soft skills with technical competencies, learners will be prepared to navigate complex organizational environments, engage diverse teams, and foster a culture of cybersecurity readiness.</td></tr>
<tr><th>Subject contents and topics</th><th>Learning outcomes (competences)</th></tr>
<tr><td rowspan="2">> Introduction to Cybersecurity

> Cybersecurity Laws and Regulations, Legal and Ethical issues in the Artificial Intelligence era

> Ethical Considerations in Cybersecurity

Information Systems Governance

> Case Studies and Practical Applications

Review and Assessment</td><td>The student is able to

- Develop effective communication strategies tailored to various stakeholders and organizational levels.

- Enhance teamwork, problem-solving, and interpersonal skills for collaboration in cybersecurity operations and projects.

- Implement systematic, evidence-based work practices to inform decision-making and improve cybersecurity outcomes.

- Design and deliver cybersecurity awareness programs that promote a positive security culture.

- Recognize and navigate the multidisciplinary aspects of cybersecurity to engage diverse expertise and perspectives.</td></tr>
<tr><td>Mapping with ENISA ECSF

Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager, Cybersecurity Architect, Cybersecurity Educator.</td></tr>
</table>

5 Conclusion

This deliverable has presented a comprehensive strategy for developing and enhancing cybersecurity skills within the European context, aligning with recognized frameworks and best practices to ensure that both current and aspiring professionals are equipped to meet rapidly evolving cybersecurity challenges. By leveraging the European Cybersecurity Skills Framework (ECSF) and integrating insights from the ECSO Minimum Reference Curriculum, the approach taken ensures that the proposed skill development program is both standards-driven and deeply attuned to market needs and organizational requirements.

The process began by establishing a clear understanding of the knowledge, skills, and competencies needed within specific cybersecurity roles. Drawing on feedback from the NG-SOC project pilot partners and mapping these needs against the ECSF provided a practical, bottom-up perspective. This led to the identification of key training modules-ranging from fundamental cybersecurity concepts to risk management, legal and regulatory compliance, auditing, and hands-on technical analysis. Critically, this modular approach allows for flexibility: the modules can be combined or adapted according to role-specific requirements, ensuring that training interventions are efficient, tailored, and directly relevant to an organization's strategic objectives.

In parallel, the considered adoption of an open-source Learning Management System (LMS), such as OpenEdX, reinforces scalability, accessibility, and adaptability. The platform's capabilities for content delivery, collaboration, assessment, and analytics support an environment where training can be continuously refined. Through data-driven insights, instructional strategies can be adjusted to better serve learner progress and organizational goals. As the needs of the cybersecurity workforce evolve-whether influenced by emerging threat landscapes, new regulations, or technological shifts-OpenEdX and the proposed training modules can be updated accordingly, ensuring that learning remains relevant and impactful.

While this deliverable focuses primarily on T5.1-establishing the strategy and foundational elements of the skill development program-it also sets the stage for T5.2. In future work, these established frameworks, curricula, and technological infrastructures will be brought to life through a hands-on educational platform and practical training exercises. This next phase will convert strategic planning into tangible learning experiences, providing learners with immersive scenarios and opportunities to practice and refine their skills in controlled, realistic environments.

In addition, the outcomes of T5.1 and T5.2 provide critical foundations for T5.3, which focuses on the development of realistic cybersecurity training and exercise scenarios. Leveraging advanced tools such as the KYPO Cyber Range Platform and immersive learning techniques, T5.3 aims to bridge the gap between theoretical knowledge and practical application, ensuring that the training program addresses real-world cybersecurity challenges effectively.

In conclusion, the objectives associated with this deliverable have been fully achieved and delivered on schedule. The groundwork laid here ensures that the subsequent implementation phase can build upon a robust, well-structured, and future-proof strategy. By integrating the ECSF, ECSO Minimum Reference Curriculum, and proven educational technologies, the project is now poised to foster a new generation of cybersecurity professionals who are both well-prepared and adaptable supporting the broader goal of strengthening Europe's cybersecurity resilience and capacity for innovation.

REFERENCES

[1] CyBOK. (2019). Retrieved November 2024, from The Cyber Security Body Of Knowledge: https://www.cybok.org/

[2] ECSO. (2017, November). Retrieved 2024 November, from Gaps in European Cyber Education and Professional Training: https://ecs-org.eu/ecso-uploads/2022/10/5fdb282a4dcbd-1.pdf

[3] ECSO. (2018). Retrieved November 2024, from Cybersecurity Awareness Trainings: A Practical Guide: https://ecs-org.eu/ecso-uploads/2022/10/5fad545d9be66.pdf

[4] ECSO. (2020, December). Retrieved November 2024, from ECSO Information and Cyber Security Professional Certification v3: https://ecs-org.eu/ecso-uploads/2022/10/60101ad752a50.pdf

[5] ECSO. (2022, December 12). Retrieved November 2024, from European Cybersecurity Education & Professional Training: Minimum Reference Curriculum: https://ecs-org.eu/ecso-uploads/2022/12/2022_SWG5.2_Minimum_Reference_Curriculum_final_v3.0.pdf

[6] ENISA. (2014, October 31). Retrieved November 2024, from Roadmap for NIS education programmes in Europe: https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe

[7] ENISA. (2015, October 19). Retrieved November 2024, from Status of privacy and NIS course curricula in EU Member States: https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-member-states

[8] ENISA. (2020). Retrieved November 2024, from Cybersecurity Skills Development in the EU: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[9] ENISA. (2022, September 19). Retrieved November 2024, from European Cybersecurity Skills Framework Role Profiles: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

[10] ENISA. (2022, September 19). Retrieved November 2024, from European Cybersecurity Skills Framework (ECSF) - User Manual: https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf

[11] European Comission. (2020, July 24). Retrieved from EU Security Union Strategy: connecting the dots in a new security ecosystem: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

[12] European Commission: Joint Research Centre. (2017). Retrieved December 2024, from DigComp 2.1:The digital competence framework for citizens with eight proficiency levels and examples of use: https://data.europa.eu/doi/10.2760/38842

[13] European Commission's Joint Research Centre. (2019). Retrieved November 2024, from A Proposal for a European Cybersecurity Taxonomy: https://publications.jrc.ec.europa.eu/repository/handle/JRC118089

[14] Merritt, M., Hansche, S., Ellis, B., Sanchez-Cherry, K., Snyder, J., & Walden, D. (2024). Building a Cybersecurity and Privacy Learning Program. Gaithersburg, MD: National Institute of Standards and Technology.

[15] Wetzel, K. (2023, June). NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce. Retrieved 2024 November, from NIST: https://doi.org/10.6028/NIST.IR.8355

NGSOC

Next Generation Security Operations Centres

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

This project has received funding from the European Union's Digital Europe Programme (DIGITAL) under grant agreement No 101145874