REWIRE
CYBERSECURITY SKILLS ALLIANCE

Co-funded by the
Erasmus+ Programme
of the European Union

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R4.2.1. WP4 REWIRE Curricula and Training Framework

Title	REWIRE Curricula and Training Framework
Document description	The document unfolds the structured plan to outline the knowledge, skills, and competencies needed for the 4 selected ENISA Occupational Profiles. It includes learning objectives, instructional materials, assessment tools, and other resources that are necessary for the successful implementation of the training program.
Nature	Public
Task	T4.2 Design and development of the REWIRE Curricula and Training Framework
Status	Draft
WP	WP4
Lead Partner	AMC
Partners Involved	URL, Apiroplus, BUT, EUC, EKT
Date	17 July 2023

CONTENTS

1. EXECUTIVE SUMMARY

The development of cybersecurity skills is critical for safeguarding digital assets, maintaining privacy, and ensuring secure online transactions. In the framework of REWIRE project a curricula and training framework is developed that aligns with the European Cybersecurity Skills Framework (ECSF) and addresses the skills gap in the cybersecurity workforce. This report provides an overview of the REWIRE curricula and training framework, the design of courses based on the framework, and outlines the best practices for creating a stakeholder network in cybersecurity education.

The framework is composed of four occupational profiles out of the twelve ENISA Occupational profiles; Cyber Incident Responder, Penetration Tester, Cyber Threat Intelligence Specialist, and Chief Information Security Officer (CISO). Each profile comprises a set of competencies, knowledge, skills, and attitudes, required to perform the job effectively. Together, these four occupational profiles cover different aspects of cybersecurity, a process that was assessed via a multi-criteria process including incident response, vulnerability assessment, threat intelligence, and strategic management. By including them in the framework, organizations can establish a well-rounded approach to cybersecurity, bolstering their defences and minimizing the potential impact of cyber threats. The framework aims to provide a structured approach to designing and delivering cybersecurity education and training that is consistent across Europe.

A multi-criteria selection method was developed and presented in this report to select the occupational profiles based on specific established criteria. The method consists of four steps: identifying the problem, evaluating the criteria, developing the score formula, selecting and weighting the criteria. The criteria for selecting the occupational profiles include the educational levels of ENISA occupational profiles, demand in the job market, available courses, stakeholders' input, level of use of the Cyber Range, and certification. The scoring formula assigns weights to each criterion, which are used to calculate the final score. The method ensures that the occupational profiles selected align with the ECSF and address the current skills gap in the cybersecurity workforce.

The design of courses based on the REWIRE curricula and training framework follows a structured approach that is in tune with the ECSF. The design process involves selecting the occupational profiles, identifying the competencies, skills, and knowledge required for each profile, and developing learning objectives based on the identified competencies. The process ensures that the courses are consistent with the ECSF and are designed to tackle the prevailing cybersecurity skills gap in the cybersecurity workforce.

The draft course outline provides an overview of the courses developed based on the REWIRE curricula and training framework for the four occupational profiles. Each course comprises a set of modules that address the knowledge, skills, and attitudes required for the specific occupational profile and are related to specific tasks. The course outline ensures that the designed materials align with the ECSF and address the skills gap in the cybersecurity

workforce. The course outline is subject to further refinement and validation to ensure that it meets the needs of the cybersecurity workforce.

Creating a stakeholder's network on cybersecurity education is critical for addressing the skills gap in the cybersecurity workforce. The stakeholder's network comprises individuals, organizations, and institutions involved in cybersecurity education and training. The best-practice guidance for creating a stakeholder's network on cybersecurity education involves defining the characteristics of the network, such as the mission, vision, goals, and objectives, identifying the stakeholders, developing communication strategies, and establishing a governance structure. The guidance ensures that the stakeholder's network is effective in addressing the skills gap in the cybersecurity workforce.

2. INTRODUCTION TO REWIRE CURRICULA AND TRAINING FRAMEWORK

As highlighted by the UNESCO International Bureau of Education[1] (2017), it is important to note that a curriculum framework is not the same as a curriculum, and the term "framework" should be carefully considered. A framework is a way of organizing and managing content, such as policies, procedures, and concepts in a systematic manner. The focus of a framework is not on the content itself, but on how the content is structured, controlled, or regulated. A curriculum framework establishes the parameters, directions, and standards for curriculum policy and practice.

Furthermore, a framework implies flexibility and allows for variation and discretion in implementation while adhering to underlying principles and standards. In the context of curriculum development, a framework should organize, control, or regulate the content of the curriculum, including subject descriptors, syllabuses, textbooks, and other learning materials. It should also encompass various aspects that affect the development and implementation of the curriculum, such as teaching methodology, assessment and examination practices, teacher recruitment and selection, class sizes, and the current and future needs of the country.

Thus, those responsible for creating a curriculum framework should consider the long-term implications and potential impact on the educational system, as well as the resources required for its effective implementation.

In the context of the REWIRE project, the Curricula and Training framework aims to provide guidance and advice on the creation of curricula and training within the cybersecurity domain. This guidance will be used by the REWIRE project in the creation of four training courses (as stipulated in the contractual project documents), which will be evaluated through the implementation of pilot iterations and will be updated and improved as needed based on the feedback received during the piloting phase. The training courses will be promoted to the cybersecurity education ecosystem.

This Curricula and Training framework should cover a range of matters that have a direct impact on the development and implementation of curriculum for cybersecurity education. This framework transcends country needs since it addresses a transnational subject: cybersecurity.

Which are the specific characteristics of cybersecurity education that need to be taken into consideration in the formulation of the REWIRE (Cybersecurity) Curricula and Training framework?

[1] Developing and implementing curriculum frameworks, by UNESCO International Bureau of Education, Document code : IBE/2017/OP/CD/02, 2017 (https://unesdoc.unesco.org/ark:/48223/pf0000250052)

The REWIRE project has carried out a PESTLE analysis[2] (Political, Economic, Social, Technological, Legal and Environmental) of factors which affect skills shortages, gaps, and mismatches, as well as impact cybersecurity education. Some of the identified challenges have a direct impact on the complexity of cybersecurity education and training and the effective development of the relevant Curricula.

Specifically, the following challenges have been identified as relevant. For each one of the identified challenges, a justification is provided:

- Lack of relevant European regulatory frameworks: In September 2022, the first European Cybersecurity Skills Framework (ECSF) was published by ENISA[3]. The ECSF describes 12 Roles of Cybersecurity professionals in Mission, Tasks, skills, knowledge, and e-competencies. Before the ECSF was published, the development of the training courses was based on the experience of the training provider, the educator, and practices from other countries or industries.
- Complexity of the cybersecurity domain and the rapid technology and threat evolution.
- Lack of dedicated curricula and training and no clear identification of skills.
- The limited existence of Cyber Ranges and other tools.
- The licensing costs and different licensing models of software in cybersecurity education.

The CONCORDIA project implemented an assessment of available cybersecurity courses provided by the project partners. The results of this assessment[4] show that:

- there is a proven heterogeneity both of cybersecurity jobs market and cybersecurity courses offer.
- there is a lack of an agreed terminology across domains and industries related to competencies needed for a specific job which makes it difficult for the companies to fill in the open positions, but also for course providers to design their curricula as to answer to the market needs, as well as for the individuals to identify the skills they need to possess or develop as to meet the requirements of the job market.

[2] Report R2.1.1 PESTLE analysis results - https://rewireproject.eu/wp-content/uploads/2022/04/R2.1.1-PESTLE-analysis-results_FINAL-v1.1_compressed.pdf

[3] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

[4] https://www.concordia-h2020.eu/wp-content/uploads/2020/04/CONCORDIA-AssessmentOfCoursesT3.4-ForWebsite.pdf

3. DESIGN OF COURSES BASED ON THE REWIRE CURRICULA AND TRAINING FRAMEWORK

3.1 Introduction to the European Cybersecurity Skills Framework (ECSF)

ENISA introduced in 2022 the European Cybersecurity Skills Framework (ECSF)[5], a practical tool that helps to identify and specify the tasks, competencies, skills, and knowledge necessary for European cybersecurity roles. It condenses all cybersecurity-related positions into 12 following role profiles:

2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)

2.2 CYBER INCIDENT RESPONDER

2.3 CYBER LEGAL, POLICY & COMPLIANCE OFFICER

2.4 CYBER THREAT INTELLIGENCE SPECIALIST

2.5 CYBERSECURITY ARCHITECT

2.6 CYBERSECURITY AUDITOR

2.7 CYBERSECURITY EDUCATOR

2.8 CYBERSECURITY IMPLEMENTER

2.9 CYBERSECURITY RESEARCHER

2.10CYBERSECURITY RISK MANAGER

2.11DIGITAL FORENSICS INVESTIGATOR

2.12 PENETRATION TESTER

Figure 1: European Cybersecurity Skills Framework ,2022 p.4

Each of the profile is analysed in detail regarding its responsibilities, skills, synergies, and dependencies. The framework establishes a mutual understanding of the essential roles, competencies, skills, and knowledge required, for European Cybersecurity professionals. It also facilitates the recognition of cybersecurity expertise, and supports the creation of cybersecurity training programs. Additionally, a user manual is included with the framework, providing practical advice on how to use it with examples and use cases. The manual offers three instances where private organizations might require cybersecurity personnel hiring, upskilling, or reskilling, along with use cases from seven organizations that applied the ECSF in diverse contexts.

[5] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

3.2 The REWIRE project and the ECSF

The European Cybersecurity Skills Framework (ECSF) of ENISA is a document of significant importance as it sets the European direction of cyber security and creates a common frame of reference for all stakeholders involved. The REWIRE project is in direct contact with ECSF utilizing its outcomes.

More specifically, in the following two deliverables of key importance for the REWIRE Curriculum and Training Framework, the ECSF was the main subject of work.

R3.2.1. Mapping the framework to existing courses and schemes

Within the framework of this deliverable, the REWIRE project suggests that in order to improve the availability, accessibility, and quality of cybersecurity courses and certifications is important to tackle the global shortage of cybersecurity experts. The report proposes the creation of a new web application, Cybersecurity Profiler, to map the required skills and knowledge for specific cybersecurity work roles as identified in the European Union Agency for Cybersecurity framework. The report describes how the web application works and its statistical analyses. The Cybersecurity Profiler can identify which courses, training, or certifications are recommended for a certain work role and create a study program, training, or certification. The report shows how to apply the methodology to existing curricula and validate it by applying it to training programmes for four specific ENISA profiles. The Cybersecurity Profiler is still in beta version and will be part of the CyberABILITY platform.

R3.2.2. Cybersecurity Skills Framework

In this deliverable, 12 profiles are included in version 0.5 of the ECSF proposed by ENISA and its relevant ad-hoc working group. Their efforts have led to an enhanced cybersecurity skills framework that addresses gaps in competencies, skills, and knowledge identified during the review of similar documents. The team's work included analyzing existing practices of ICT-03 pilots such as CONCORDIA, ECHO, CyberSec4Europe, and SPARTA, reviewing information within the profiles, examining existing information from other national and international cybersecurity skills frameworks, correlating the profiles to identify gaps, rephrasing the tasks using specific action words and standardized language, correlating each task to the required knowledge, skills, and competencies, and reviewing the ESCO skills and knowledge taxonomies to identify and add non-digital skills and knowledge. The results of the team's efforts are presented in the REWIRE Cybersecurity Skills Framework, which is compared to ENISA's proposal for ECSF v0.5.

3.3 Development of the Multi-criteria Method for Occupational Profile selection

The methodology for selecting the occupational profiles is a crucial element in bridging the gap between the current state of cybersecurity education and the demands of the job market. REWIRE proposes a multi-criteria selection method to ensure that the selected profiles meet the following objectives.

Objectives

There is an insufficient number of cybersecurity specific multidisciplinary curricula which would offer fundamental skills necessary for cybersecurity education. According to ENISA[6], the key issues with curricula are outdated or unrealistic platforms in education environments, difficulties in keeping pace with the outside world, lack of qualified cybersecurity educators, poor interaction with the industry, and disconnection to the labour market needs. These aspects could be further extended to lack of hands-on experience, which is pivotal in cybersecurity domain and balancing up-to-date information with the foundation of transferable skills that graduates can build on and can further extend in their careers. Moreover, employees are not being offered an adequate level of training, which is crucial for keeping pace with constant innovation in the industry and it is especially important for junior or mid-level professionals, who need to further develop their specialized knowledge in cybersecurity. In addition, there are no educational institutions, promoting cybersecurity as one of the key specializations in their portfolio. Cybersecurity remains a narrow specialization, not communicated as an attractive profession for diverse groups of young people.

Examples of possible effects on cybersecurity are:

- Lack of applicants for cybersecurity degrees.
- Mismatch between industry expectations and skills of graduates (qualitative issue).
- Shortage of qualified cybersecurity professionals (quantitative issue).

Specific Objectives:

[O1] To ensure high-quality standards of the training material.

[O2] To meet the current and future needs and developments in the field of cybersecurity.

[O3] To reach out to a wide range of participants and ensure that they benefit from the designed training courses.

[6] https://www.enisa.europa.eu/

Criterions

The first objective (O1) aims to guarantee the high quality of training materials. Criterion A, which examines the educational levels of ENISA Occupational Profiles, ensures that the materials cater to different levels of expertise, promoting comprehensive understanding and depth of knowledge. Additionally, Criterion C prevents redundancy in course design and ensures the inclusion of relevant and up-to-date information.
The second objective (O2) focuses on meeting the current and future needs of the cybersecurity industry. Criterion B considers job market demand, aligning the courses with industry requirements. Criterion D gathers input from stakeholders to ensure the courses meet their needs and expectations. Criterion E incorporates practical exercises on the Cyber Range, reflecting evolving trends and developments.
Lastly, the third objective (O3) centers on accessibility and benefit to a wide range of participants. Criterion A ensures the courses are accessible to learners with different expertise levels, while Criterion C offers diverse options tailored to participants' needs. Criterion F ensures the provided certification is widely recognized, promoting professional growth and career advancement for participants.
This is the list of the 6 criterions selected:

- **CRITERION A – Educational Levels of ENISA Occupational Profiles** [*O1*, *O3*]
- **CRITERION B – Demand of The Job Market** [*O2*]
- **CRITERION C – Already Available Courses** [*O1*, *O3*]
- **CRITERION D – Stakeholders' Input** [*O2*]
- **CRITERION E – Hands-on exercises on the Cyber Range** [*O2*]
- **CRITERION F – Certification** [*O3*]

In this stage, weights were assigned to each of the criteria to indicate their relative importance, summarized in three levels: "Heavy," "Medium," and "Light." To ensure the reliability of the results, a sensitivity analysis was conducted, testing the scoring formula with different scores and varying the weights of the criteria or the scores of the Occupational Profiles. This comprehensive process of input gathering, formula development, weight discussion, and sensitivity analysis emphasizes the importance of collaboration, transparency, and robustness in the evaluation process.

3.4 Implementation of the Multi-criteria Method for Occupational Profile selection

The final Multi-Criteria Selection Method was parted by six criteria and a Score Formula applying weights for each criterion, and two control measures (a second score and a screening index tool). After considering the above-mentioned preceding steps, six final criteria have been chosen. In this section, we present these criteria along with their rationale and the objectives they fulfil.

3.4.1 Criterion A – Educational Levels of ENISA Occupational Profiles

This criterion takes into consideration of the educational levels of where the ENISA Occupational Profiles' competencies rank.

Rational and Objectives

This criterion serves REWIRE's aim to provide training material responding to different EQF (European Qualifications Framework) levels. The inclusion of professionals and students with low educational requirements is considered particularly important, as it would allow:

- more participants to be enrolled.
- less participants to drop out due to lack of their ability to respond to the needs of the trainings.
- develop a wider range of activities.
- deliver training material that would further escalate the competencies of the trainees.

Based on the above Criterion A is to examine the EQF levels of each Occupational Profiles.

Specific Objectives:

- ✓ The high-quality standards of the training material to be created.
- ✓ The job market and academic / VET trends.
- ✓ Reaching and benefiting a wider range of participants.

Methodology and Scoring

The educational levels of each profile are to be linked with EQF levels. Since each profile is present to more than one level, the input to the criterion will be in ranges (for example; EQF 2/3/4, EQF 4/5). Emphasis will be given on both the entry level (lowest of the range) as well as the width of the range. Based on that the profiles present in the lowest levels and in the most levels are to be given higher scores, while the others will be given lower scores. The following section is also linked with the e-competences identified in a previous stage (R3.3.1) of the REWIRE project.

The score for each Occupational Profile will vary from 1 to 5 based.

The Criterion was given "heavy" weight, as it was considered quite important for the final decision.

Input – Engagement level of partners

The main input to this Criterion was based on the results of R3.3.1. "Cybersecurity Skills Framework".

ENISA Occupational Profiles	EQF levels
CHIEF INFORMATION SECURITY OFFICER (CISO)	4/ 5
CYBER INCIDENT RESPONDER	2/ 3/ 4
CYBER LEGAL, POLICY & COMPLIANCE OFFICER	3/ 4
CYBER THREAT INTELLIGENCE SPECIALIST	3/ 4
CYBERSECURITY ARCHITECT	3/ 4

CYBERSECURITY AUDITOR	3/ 4
CYBERSECURITY EDUCATOR	2/ 3
CYBERSECURITY IMPLEMENTER	2/ 3
CYBERSECURITY RESEARCHER	2 /3 /4 /5
CYBERSECURITY RISK MANAGER	3/ 4
DIGITAL FORENSICS INVESTIGATOR	3/ 4
PENETRATION TESTER	2/3 /4

3.4.2 Criterion B – Demand of the job market

This criterion takes into account the demand in online job advertisements at EU level.

Rational and Objectives

Identifying the ENISA profiles at the most demand in the job market, will allow to develop training materials to upskill and reskill professionals and students able to cover the job positions in need. This way, we aim to increase the pool of suitable candidates and successfully respond to the needs of the market regarding the field of cybersecurity. Addressing the job market's needs, will increase on one hand the demand of the training among individuals and on the other hand it will be proven useful to the companies to use the REWIRE curricula and trainings to upskill and reskill their staff internally (following among other the new trend in human resource, "Quiet Hiring").

Specific Objectives:

- ✓ The current and future real needs and developments in the field of cybersecurity.
- ✓ The job market and academic / VET trends.
- ✓ Reaching and benefiting a wider range of participants.

Methodology and Scoring

The core principle of the methodology was to analyze the demand of the job market at EU level. It was decided to use job ads on the web. As the job titles between every company, sector, or country, differ to those of the ENISA Occupational Profiles, the team set the matching based on the requirements and skills described in each add in order to create specific materials.

The score for each Occupational Profile is varied from 1 to 5 based on the number of job ads linked to it. Based on the distribution of the number of ads per profile, different tiers would be formed, as a secondary scoring system for each criterion with different tiers assigning different scores with the higher tiers to give a higher score to the profiles entering in, and the lower tiers give lower score accordingly.

Due to the nature of the chosen ads, the criterion was labelled as "lightweight". The sample size was substantial, yet it wasn't deemed representative enough to offer compelling support or reach meaningful conclusions. Therefore, in the entire evaluation process, this factor is

given less weight and/or value. It is crucial to take into account the restrictions of the chosen ads and acknowledge that they might not fairly depict the total populace or offer a complete picture of the circumstance.

Input – Engagement level of partners

The REWIRE Cybersecurity Job Ads Analyzer (WP3), was used as the main source of the criterion.

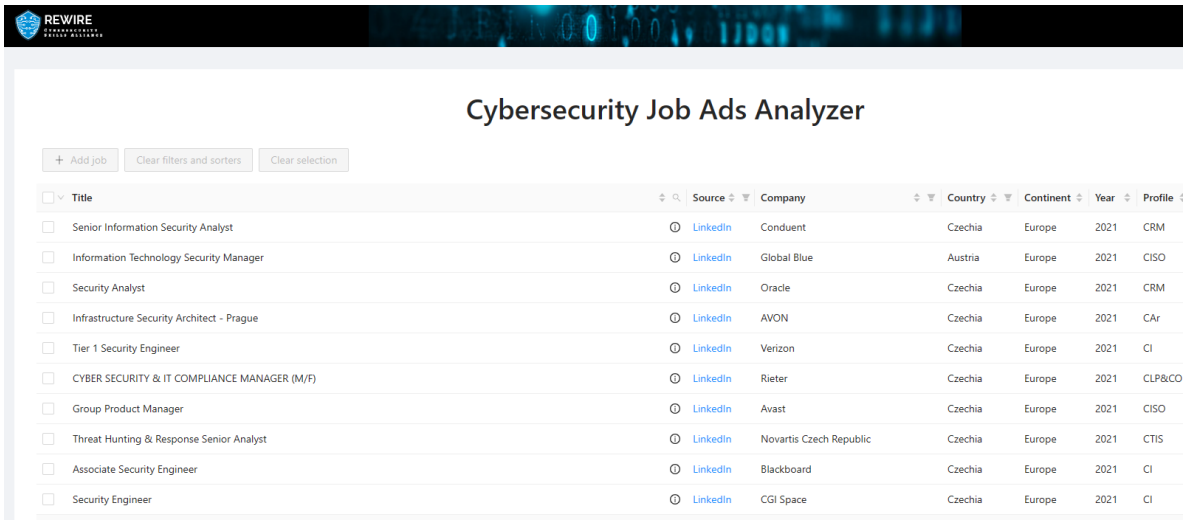


Figure 3:The Cybersecurity Job Ads Analyzer in the framework of REWIRE project

for more information: https://rewire.informacni-bezpecnost.cz/

358 job ads at the REWIRE's database were linked to the 12 ENISA Occupation Profiles, demonstrating EU's job market needs. It is important to note that 9 job ads, did not match to any of the 12 profiles.

	ENISA Occupational Profiles	Total Number
1	Cybersecurity Implementer	93
2	Cybersecurity Architect	50
3	Cyber Incident Responder	47
4	Chief Information Security Officer (CISO)	32
5	Cyber Threat Intelligence Specialist	31
6	Penetration Tester	25
7	Cybersecurity Risk Manager	24
8	Cyber Legal, Policy & Compliance Officer	19
9	Cybersecurity Auditor	15
10	NA	9
11	Cybersecurity Researcher	6
12	Cybersecurity Educator	4
13	Digital Forensics Investigator	3
Total		**358**

Based on the above the Tiers were formed as below:

TIER	RANGE	SCORE
TIER S	> 50	5
TIER A	> 40	4
TIER B	> 30	3
TIER C	> 10	2
TIER D	< 10	1

The tires were established based on the scores assigned to each profile, which were determined by the number of job ads linked to them. The distribution of the number of ads per profile allowed for the formation of different tiers. Profiles that had a higher number of job ads linked to them were placed in the higher tiers, while profiles with a lower number of job ads were placed in the lower tiers. By using these tiers, a clear distinction was made to highlight the varying levels of importance and demand for each profile within the cybersecurity field.

3.4.3 Criterion C – Already Available Courses

Criterion C refers to the number of the existing curricula and trainings available for each of ENISA Occupational Profiles.

Rational and Objectives

Inter alias, the main aim of the REWIRE project is to cover training gaps in the field of cybersecurity. Although, that we are to introduce innovative and effective training methods through the REWIRE courses, at the same time we addressed as important to not deliver courses and training material, similar to existing ones. To develop training programs, materials, and resources that meet the objectives of REWIRE project a thorough search was conducted. Based on this research, specific courses that match the chosen occupational profiles are developed that meet the needs and restrictions of the market as well as it was taken into account the lack or limited materials about these specific Occupational Profiles.

Specific Objectives:

- ✓ To develop materials considering the market's need and the current academic / VET trends.
- ✓ To Reach out and benefit a wider range of participants.

Methodology and Scoring

Similar to Criterion B, the core principle of the methodology was to map the available courses at EU level. Both curricula and trainings, were to be found and matched with the 12 ENISA Occupational profiles, based on the competences they were covering.

Depending on the amount of curricula and trainings connected to each Occupational Profile, a score between 1 and 5 is given. The number of curricula and trainings offered for each profile determines how the points are distributed across the various tiers. The profiles

featured in higher tiers receive greater ratings, while those in lower levels receive lower marks. Finally, each occupational profile is given an average score (rounded up). The Criterion was given "light" weight. Two factors led to that decision.

The REWIRE trainings should be developed regardless of the amount of current trainings for any of the occupational profiles. The employment of cutting-edge training techniques and resources had an impact on this choice, highlighting how crucial it is to develop the REWIRE trainings despite the existence of other training options for the particular professional profiles. It was jointly recognized by all partners that the sample size, although indicative, was not sufficiently large for the criterion to be given greater weight.

Input – Engagement level of partners

Capitalizing the work done during the previous stages and especially WP3, following inter alias the cost-effectiveness scope of the project, the R3.4.1 "Mapping the framework to existing courses and schemes" is used.

Curricula

ENISA OPs	1	2	3	4	5	6	7	8	9	10	11	12
Result (median)	46%	38%	80%	60%	78%	50%	75%	75%	56%	71%	67%	50%

TIER	RANGE	SCORE
TIER S	< 40%	5
TIER A	41% to 50%	4
TIER B	51% to 70%	3
TIER C	71% to 75%	2
TIER D	> 76%	1

Trainings

ENISA OPs	1	2	3	4	5	6	7	8	9	10	11	12
Result (median)	8%	13%	20%	10%	22%	0%	0%	13%	11%	14%	17%	0%

TIER	RANGE	SCORE
TIER S	0%	5
TIER A	1% to 10%	4
TIER B	11% to 15%	3
TIER C	16% to 20%	2
TIER D	> 21%	1

3.4.5 Criterion D – Stakeholders' Input

The criterion referred to the input of all partners, capitalizing the wide expertise of the consortium and the experts involved in the project development.

Rational and Objectives

Respecting all partners' expertise as well as the fact that all are to contribute to the development of the training material, all partners were asked to grade the 12 ENISA Occupational Profiles based among others on:

a) Their input as representatives of the academia, VET, job market, and their knowledge regarding the importance of each profile. The REWIRE consortium consists of a wide range of professionals, directors, heads of programs or projects, who are in position to provide a trustworthy input regarding the market trends, the gaps and upcoming development in the field of cybersecurity, the interest of university students and VET learners etc.

b) Their capacity for the course content creation, and their expertise regarding the ENISA Occupational profiles.

This would lead to choose on one hand Occupational profiles that would respond to real needs, while on the other ensure that the training material created would be of high quality.

Specific Objectives:

- ✓ To create high-quality standards of the training material.
- ✓ To underline the current and future real needs and developments in the field of cybersecurity.
- ✓ To act according the job market and academic / VET trends.
- ✓ To Reach out and benefit a wider range of participants.

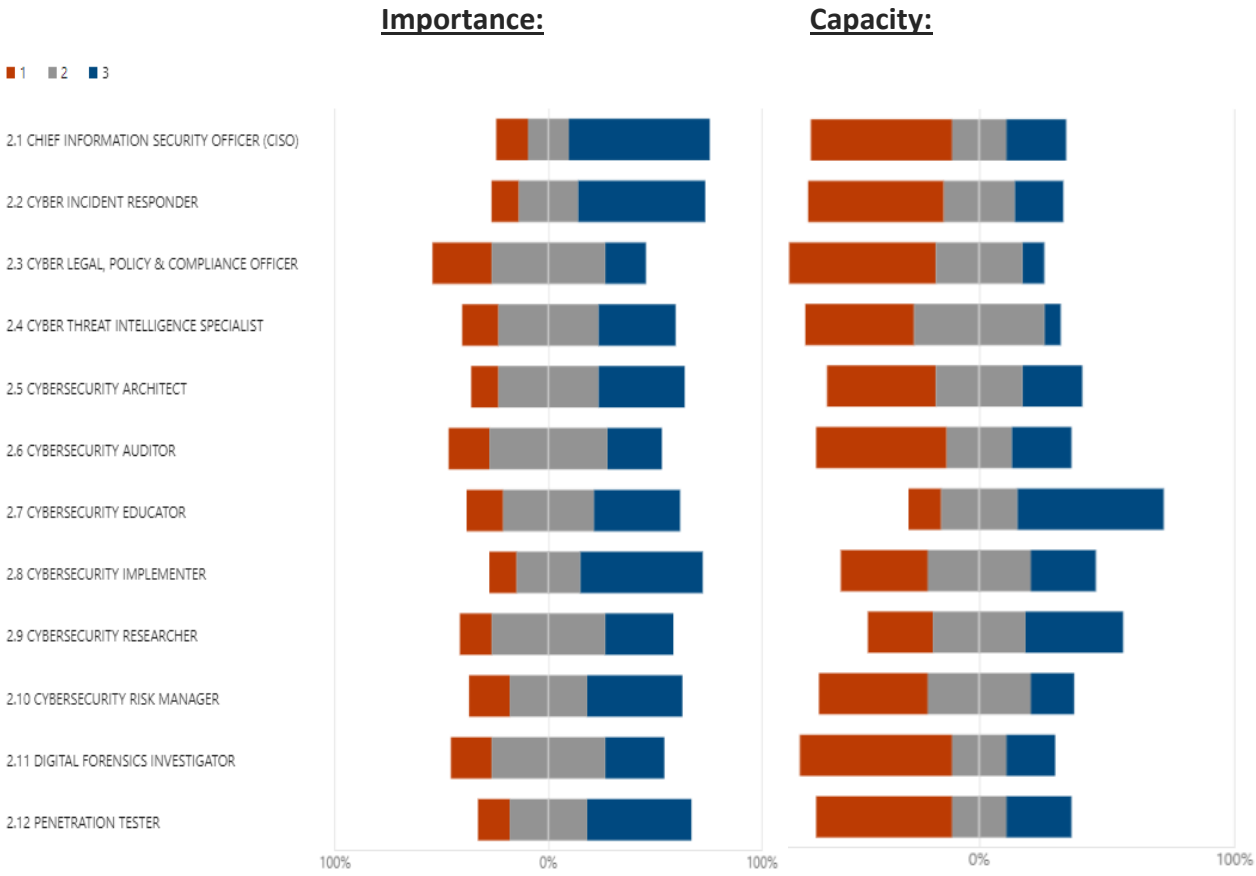
Methodology and Scoring

The Criterion was given "Heavy" weight, as it was strictly and highly related to all the specific objectives of the methodology.

Input – Engagement level of partners

Up to 47 stakeholders among the partnership gave their insights and professional opinion regarding the importance of each profile. The total consortium also evaluated their capacity. Below we present the charts of the responses:

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe



3.4.6 Criterion E - Level of use of the Cyber Range

This criterion reflects the use and capitalization of the Cyber Range in the training materials.

Rational and Objectives

The Cyber Range developed within the framework of the REWIRE project, is considered the major innovative element of the proposed REWIRE training methodology. It presents a unique training tool, which is linked to the quality of the training material. The use of Cyber Range is to design and establish a curriculum and training framework characterized by practical activities and supporting real case scenarios meeting on one hand the needs of the job market as well as the modern pedagogical approaches of the academia and the VET sector. In addition, will contribute to the creation of an interactive training, appealing to the learners, regardless their status (professionals or students), and leading to larger number of participants.

Specific Objectives:

- ✓ To create high-quality standards of the training material. To act according the job market and academic / VET trends.
- ✓ To Reach out and benefit a wider range of participants.

Methodology and Scoring

For the evaluation of the ENISA Occupational profiles, we used a 3 Tier list based on the table below.

Use of Cyber Range	Explanation	Score
CR is essential for the training.	• Profile is focused on technical tasks. • Practical knowledge of offensive/defensive tools is necessary	5
CR is somehow important for the training.	• Profile's focus is mixed between technical tasks and policies/management. • Practical knowledge of offensive/defensive tools is beneficial.	3
CR is unnecessary for the training.	• Profile is focused on policies and management • Theoretical knowledge of offensive/defensive tools is sufficient	1

Criterion E was given "Heavy" weight, based on the innovation it brings to the Curricula and Training Framework, as well as its key role to the project.

Use of Cyber Range	ENISA Occupational Profiles
CR is essential	2.2 CYBER INCIDENT RESPONDER 2.11 DIGITAL FORENSICS INVESTIGATOR 2.12 PENETRATION TESTER
CR is important	2.4 CYBER THREAT INTELLIGENCE SPECIALIST 2.5 CYBERSECURITY ARCHITECT 2.6 CYBERSECURITY AUDITOR 2.7 CYBERSECURITY EDUCATOR 2.8 CYBERSECURITY IMPLEMENTER 2.9 CYBERSECURITY RESEARCHER
CR is unnecessary	2.1 CHIEF INFORMATION SECURITY OFFICER (CISO) 2.10 CYBERSECURITY RISK MANAGER 2.3 CYBER LEGAL, POLICY & COMPLIANCE OFFICER

3.4.7 Criterion F – Certification

Criterion F measures the number of the existing certifications they exist for each of ENISA Occupational Profiles.

Rational and Objectives

Considering the REWIRE Trainings are connected to specific certification schemes, it is crucial for the project to consider the existing certifications associated with each of the 12 ENISA Occupational Profiles. The project aims to avoid adding another certification to the numerous ones already available for each Occupational Profile. Instead, the focus is on offering training options for profiles with limited certification opportunities. This approach addresses a specific market and academic/VET field gap while making the training more appealing compared to others. Thus, mapping the certifications is an important criterion that holds value and should be given due consideration.

Specific Objectives:

- ✓ To underline the current and future real needs and developments in the field of cybersecurity.
- ✓ To create high-quality standards of the training material. To act according the job market and academic / VET trends.
- ✓ To reach out and benefit a wider range of participants.

Methodology and Scoring

The methodology was developed around two main factors:

a) The ability for the profiles to develop and put in action a well-established and reliable certification scheme.
b) Identifying a certain number of certifications at EU level and match them to the ENISA Occupational profiles. Each certification would be possible to be linked with more than one Occupational Profiles, as it is possible to be cover a wider range of roles and competences.

In the case, an Occupational Profile could not meet the first factor, it would be scored with. The other profiles would be divided in Tiers and be scored from 1 to 5.

Criterion E was given “medium” weight, based on the innovation it brings to the Curricula and Training Framework, as well as its key role to the project.

Input – Engagement level of partners

Firstly, the CYBERSECURITY EDUCATOR role involves teaching cybersecurity concepts and practices to others. However, there are already certifications available for teaching and education. These certifications cover the skills and knowledge required for effective teaching, including the ability to design curriculum, assess student learning, and manage classroom environments. While these certifications do not specifically focus on cybersecurity, they still demonstrate proficiency in the fundamental principles of education, which are essential for any cybersecurity educator.

Secondly, the CYBERSECURITY RESEARCHER role involves investigating and exploring new and emerging cybersecurity threats and technologies, which can be highly abstract and complex. It can be challenging to define a specific set of skills or knowledge required for this role, and a certification scheme may not accurately capture the depth and breadth of a researcher's expertise. Furthermore, cybersecurity research often involves interdisciplinary collaboration and innovation, making it difficult to develop a certification that accurately reflects the diverse skill sets required for this role.

In conclusion, the roles of CYBERSECURITY EDUCATOR and CYBERSECURITY RESEARCHER are not well-suited for a certification scheme, as the certifications already available for education cover the necessary skills, and the abstract and interdisciplinary nature of cybersecurity research makes it challenging to develop a meaningful certification for researchers.

On a second stage, based on Security Certification Roadmap 60 certifications were selected and linked to the 10 other ENISA Profiles.

ENISA Occupational Profiles	Number of Certifications linked to them
CHIEF INFORMATION SECURITY OFFICER (CISO)	5
CYBER INCIDENT RESPONDER	3
CYBER LEGAL, POLICY & COMPLIANCE OFFICER	4
CYBER THREAT INTELLIGENCE SPECIALIST	6
CYBERSECURITY ARCHITECT	3
CYBERSECURITY AUDITOR	7
CYBERSECURITY IMPLEMENTER	16
CYBERSECURITY RISK MANAGER	1
DIGITAL FORENSICS INVESTIGATOR	13
PENETRATION TESTER	10

Based on the above the Tiers were formed as below:

TIER	RANGE	SCORE
TIER S	1 to 2	5
TIER A	3 to 5	4
TIER B	6 to 10	3

TIER C	Over 10	2
TIER D	N/A	1

Consideration of this criterion is crucial to ensure the development of a training program that effectively caters to the requirements of learners and the job market. The methodology employed to map certifications to the ENISA Occupational Profiles encompassed two key factors. Primarily, the evaluation focused on the profiles' capacity to establish and execute a reliable certification scheme. By assessing this aspect, the aim was to ensure that the selected certifications align with the profiles in a manner that promotes trustworthiness and credibility within the cybersecurity domain.

3.5 Scoring Formulas

As described in 2.1 it was decided to use two scores. The first score was to be a result of a scoring formula based that would take into consideration the weights, as set by the partners, the second based on the average score of each Profile in all criteria.

Last but not least a screening index was to be used to identify and set under further investigation Occupational Profiles with high scoring because of extremely high and extremely low scores on specific criteria.

Weighted Score

The “weighted score” is the result of adding the scores each Occupational Profile was given for each criterion based on its specific methodology and multiplied by its weight. Scores with “Light” criteria were multiplied by 1, scores with “Medium” criteria were multiplied by 1.5, and scores with “Heavy” criteria were multiplied by 2. Below the formula is presented:

$$OPscore = \text{“}Criterion\_a\text{”}\ x\ \text{“}weight\_heavy\text{”} + \text{“}Criterion\_b\text{”}\ x\ \text{“}weight\_light\text{”} + \text{“}Criterion\_c\text{”}\ x\ \text{“}weight\_light\text{””} + \text{“}Criterion\_d\text{”}\ x\ \text{“}weight\_heavy\text{”} + \text{“}Criterion\_e\text{”}\ x\ \text{“}weight\_heavy\text{”} + \text{“}Criterion\_f\text{”}\ x\ \text{“}weight\_medium$$

Or

$$OPscore = 2xCriterion\_a + Criterion\_b + Criterion\_c + 2xCriterion\_d + 2xCriterion\_e + 1.5xCriterion\_f$$

Average Score

The average score is the result of adding the scores each Occupational Profile was given for each criterion based on its specific methodology, divided by the number of Criteria, without taking into consideration their weights.

$$AVScore = \frac{(Criterion\ a + Criterion\ b + Criterion\ c + Criterion\ d + Criterion\ e + Criterion\ f)}{number\ of\ criteria}$$

3.6 REWIRE Final Selection

After collecting all the results from the engaged partners, following the specific methodologies for each criterion set, we used the above formulas to review the results of each score and interpret them in the context of the decision making. We used the results to identify the best options and make the final decision about which option to choose.

ENISA Occupational Profiles	Criterion A	Criterion B	Criterion C	Criterion D	Criterion E	Criterion F
CHIEF INFORMATION SECURITY OFFICER (CISO)	2	3	4	5	1	4
CYBER INCIDENT RESPONDER	5	4	4	4	5	4
CYBER LEGAL, POLICY & COMPLIANCE OFFICER	3	2	2	1	1	4
CYBER THREAT INTELLIGENCE SPECIALIST	4	3	4	2	3	3
CYBERSECURITY ARCHITECT	3	4	1	3	3	4
CYBERSECURITY AUDITOR	4	2	5	2	1	3
CYBERSECURITY EDUCATOR	1	1	4	5	3	1
CYBERSECURITY IMPLEMENTER	1	5	3	4	3	2
CYBERSECURITY RESEARCHER	5	1	3	3	3	1
CYBERSECURITY RISK MANAGER	3	2	3	2	1	5
DIGITAL FORENSICS INVESTIGATOR	4	1	3	1	5	2
PENETRATION TESTER	5	2	5	3	5	3

Based on the above the Occupational profiles with the highest scores were formed as presented below (sorted by the highest score to the lowest):

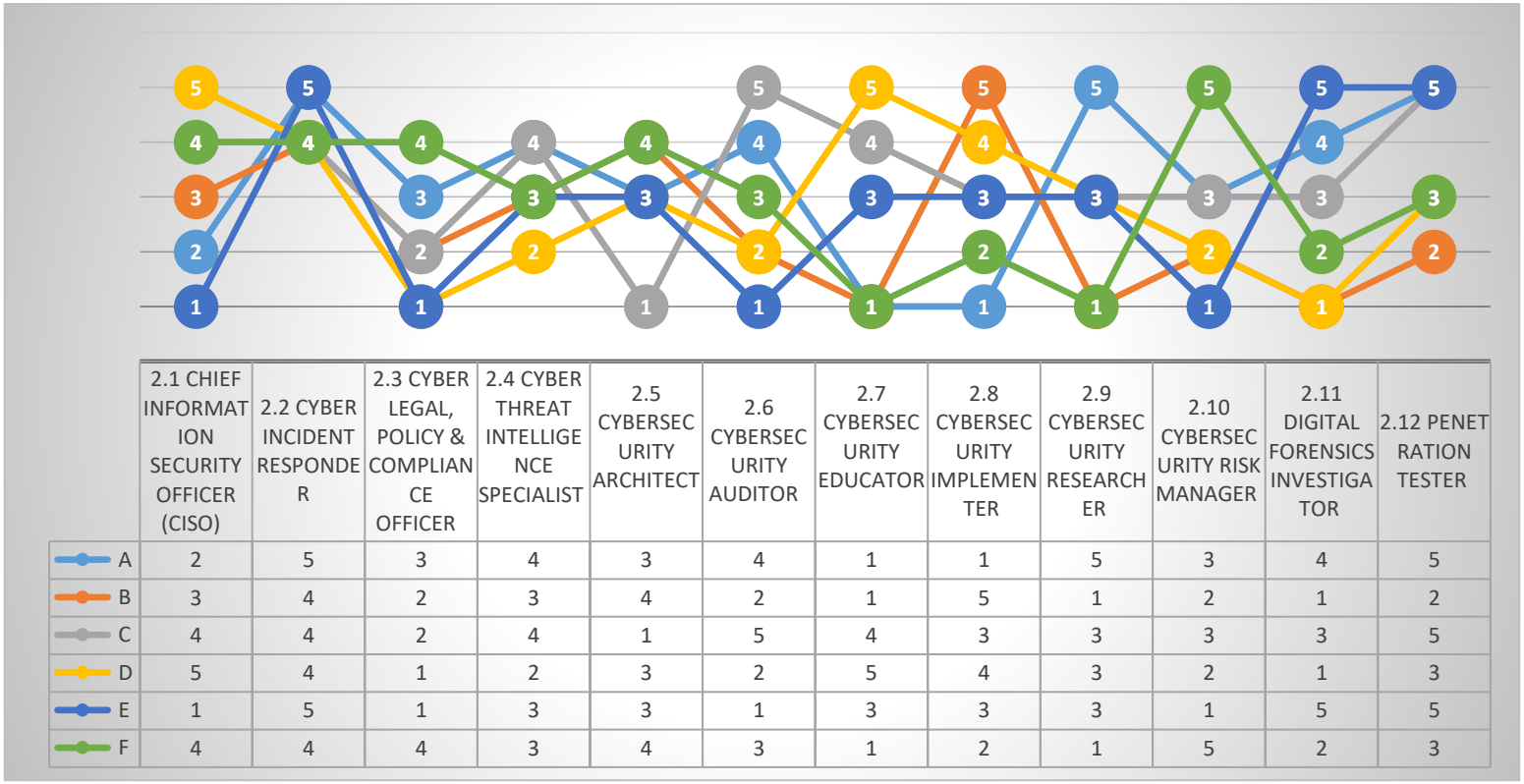
ENISA Occupational Profiles	Weighted Score	AV Score
CYBER INCIDENT RESPONDER	42	4.3
PENETRATION TESTER	37.5	3.8
CYBER THREAT INTELLIGENCE SPECIALIST	29.5	3.2
CHIEF INFORMATION SECURITY OFFICER (CISO)	29	3.2
CYBERSECURITY ARCHITECT	29	3.0
CYBERSECURITY RESEARCHER	27.5	2.7

CYBERSECURITY IMPLEMENTER	**27**	**3.0**
DIGITAL FORENSICS INVESTIGATOR	**27**	**2.7**
CYBERSECURITY AUDITOR	**25.5**	**2.8**
CYBERSECURITY EDUCATOR	**24.5**	**2.5**
CYBERSECURITY RISK MANAGER	**24.5**	**2.7**
CYBER LEGAL, POLICY & COMPLIANCE OFFICER	**20**	**2.2**

At first, the occupational profiles were examined based on their Weighted Score. As the 2.1 CHIEF INFORMATION SECURITY OFFICER (CISO) and the 2.5 CYBERSECURITY ARCHITECT, shared the same Weighted Score, the AV score was used to break the tie.

Finally, the screening index was examined to check if the final Occupational profiles; 2.2 CYBER INCIDENT RESPONDER, 2.12 PENETRATION TESTER, 2.4 CYBER THREAT INTELLIGENCE SPECIALIST, 2.1 CHIEF INFORMATION SECURITY OFFICER (CISO) presented significant differences between the criteria.

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe



	2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)	2.2 CYBER INCIDENT RESPONDER	2.3 CYBER LEGAL, POLICY & COMPLIANCE OFFICER	2.4 CYBER THREAT INTELLIGENCE SPECIALIST	2.5 CYBERSECURITY ARCHITECT	2.6 CYBERSECURITY AUDITOR	2.7 CYBERSECURITY EDUCATOR	2.8 CYBERSECURITY IMPLEMENTER	2.9 CYBERSECURITY RESEARCHER	2.10 CYBERSECURITY RISK MANAGER	2.11 DIGITAL FORENSICS INVESTIGATOR	2.12 PENETRATION TESTER
A	2	5	3	4	3	4	1	1	5	3	4	5
B	3	4	2	3	4	2	1	5	1	2	1	2
C	4	4	2	4	1	5	4	3	3	3	3	5
D	5	4	1	2	3	2	5	4	3	2	1	3
E	1	5	1	3	3	1	3	3	3	1	5	5
F	4	4	4	3	4	3	1	2	1	5	2	3

Based on the screening index, none of the final Occupational profiles present worrying differences between their score.

4. THE REWIRE CURRICULA AND TRAINING FRAMEWORK

The REWIRE Curricula and Training Framework is a comprehensive guide that outlines the objectives, structure, total hours, and training methods to be used for the development of the trainings and training material for the selected ENISA Occupational Profiles. It serves as a roadmap for all the partners involved, ensuring that everyone involved in the training process is on the same page and understands what is expected of them.

The training aim and learning objectives of the program will be defined, providing a clear understanding of what participants is expected to gain from completing the training. The training aims and learning objectives follow the need analysis (R2.2) as it was implemented during WP2 and its results. They also follow the EQF levels set for each Occupational profile. Developers of the training are to use them during the selection and the creation of the training material (definitions, concepts, knowledge, case studies, examples, exercises, cyber exercise scenarios, self-evaluation schemes).

The REWIRE Curricula and Training Framework also describes the structure of the programs, including the number of Modules and the topics that will be covered and the sequence in which they will be presented. The training program's total hours are also specified, along with the time commitment required from participants. Also, the Curriculum and Training Framework indicates the training methods agreed to be used to deliver the training.

4.1 From Skills and Knowledge to learning objectives

The first step of designing the REWIRE learning experience, was to start with a clear understanding of what skills and knowledge needed for the learners to acquire to respond to the needs of the selected Occupational Profiles. This was the main subject of previous deliverables of the project (R2.2.1, R2.2.2, R2.2.3, R3.2.1, R3.3.1, R3.4.1, 3.5.1).

Based on the above the REWIRE project has extend its capacity and be in position to develop specific learning objectives to guide the development of the REWIRE training materials and assessments.

4.2 The draft Courses Outline

The aim of the REWIRE trainings is to ensure that learners will be engaged to the training and make the most out of the given training material. We expect, through interactive exercises introduced through the use of the Cyber Range to apply an active e-learning model, for the benefit of the learners (increased competences, enhanced motivation to seek extra learning opportunities). At the same time, we want to avoid any discrimination and deliver trainings aiming at a wide range of professionals and student. This aim is not limited to learners accessing the training, but also to minimize the dropout rates among those learners who will be enrolled to the trainings, yet they will not complete the training.

Cybersecurity is a complicated scientific field. Learners need to meet preliminary requirements to successfully follow all the training. For example, they need to have good knowledge of English, adequate digital skills such as basic knowledge of programming or knowledge about cyber security, and basic knowledge in other fields such as the way a company or a team is structured in order to understand the concepts and fields of application of the cybersecurity.

Informing the potential learners about the preliminary requirements before their enrolment in the training is not considered a good practice. Many times, the learners are not able to successfully self-evaluate their own skills. They either underestimate their competencies or get discouraged deciding not to be enrolled in a training, or they overestimate their competencies and find themselves in a training that they cannot follow leading them to drop out without completing it. There are also learners, who manage to complete a training benefiting to the minimum, although in the case they would have received a brief preparation session they would be able to take advantage of the training and benefit way more by the learning opportunity they gave to themselves.

Based on the above we have decided to include a pre-survey to all four trainings and allow the learners to have a clearer picture whether they can or not complete the trainings. Moreover, each training will include a Preparatory Training, including basic and horizontal knowledge and information about the field of cybersecurity. Preparatory Training will be either optional or mandatory based on the results of the pre-survey.

The results of the pre-survey will lead to three different results and inform the learners accordingly:

- In the case they will not meet the preliminary requirements, they will be encouraged to develop their skills and competences. If possible, the survey will suggest to them

about specific trainings (based on the R3.4.1) they can follow before being able to join the training

- In the case they lack a good knowledge of the field of cyber security they will be automatically enrolled in the training, yet the Preparatory Training (Module 0), will be mandatory to them. Learners who will have specific gaps to some of the topics, only these topics will be mandatory to them, while the others will be optional.
- In the case the learners will present an adequate level of knowledge, meeting all prelaminar requirements, they will be automatically enrolled to the training and the Preparatory Training (Module 0) will be open to them optionally.

Preparatory Training is also linked with a series of additional learning benefits that will lead to a better quality of the training. Inter alias, it allows the learners to:

- Improve their skills: Preparatory training can help learners improve their skills, which are essential for the successful completion of any training.
- Fill knowledge gaps: Preparatory training can help learners fill in any knowledge gaps they may have in a particular subject area, ensuring they are adequately prepared to begin their formal studies.
- Adapt to learning expectations: Preparatory training can help learners better understand the learning outcomes and objectives of the training. They can also redefine their own learning goals and what they expect from the training and themselves during the learning procedure. Learners who follow a Preparatory Training are more motivated after its completion and tend to focus on specific parts of the training based on their needs and personal learning objectives.
- Get familiar with the learning environment: Preparatory training can provide learners with an opportunity to get familiar with the learning environment allowing them to use better the cyber range and be more active through it from the beginning.
- Improve confidence: Preparatory training can help learners feel more confident and prepared as they begin training, reducing anxiety and improving academic performance.

4.2.1 Occupational Profile 1 - CYBER INCIDENT RESPONDER

CYBER INCIDENT RESPONDER
TRAINING AIM
The aim of the training is to introduce the learners to the role of Cyber Incident Responder and increase their capacity to meet its main tasks. The educational material combines a good theoretical framework and innovative interactive e-learning methods, with emphasis to the use of a Cyber Range and the execution of specific cyber exercise scenarios. The training will be linked to a certification examination providing the learners with a formal recognition for the level of competencies they will have in the field of cybersecurity and the specific role of the Cyber Incident Responder

CYBER INCIDENT RESPONDER		
PROGRAMME OBJECTIVES		
By the end of this course, learners will acquire or develop specific knowledge, skills and attitudes which will allow them to investigate, analyse, and respond to cyber incidents within the network environment. The main competences of the course will unfold according to the revised ENISA Occupational Profile of the Cyber Incident Responder, as introduced within the framework of the REWIRE project (WP2) Learners will be able among others to monitor the system including the infrastructure and the services for anomalies, performs preventive actions to mitigate vulnerabilities and corrective actions such as to mitigate the impact of cyber incidents. They will also be in position to identify threats and root causes of incidents, collects evidence, documents the incidents and actions taken, and develops strategies for avoiding future incidents.		
Knowledge	**Skills**	**Attitudes**
• Aware of intrusion detection methodologies and techniques for detecting host and network-based intrusions • Know of network security architecture concepts including topology, protocols, components, and principles • Understand the OSI (Open Systems Interconnection) model and underlying network protocols (e.g., TCP/IP) • Have knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name	• Performing damage assessments • Securing network communications • Use security event correlation tools • Identify, Capture, contain, and report malware • Recognize and categorize types of vulnerabilities and associated attacks • Handle effectively available methodologies	• Recognize the importance of regular assessments • Value the benefits of a secure network to the smooth operation of a company • Willing to continuously be updated in newly introduced threats • Carefully perform duties • Be eager to address any i on time

System (DNS), and directory services • Discover different classes of attacks and cyber-attack stages • Describe system and application security threats and vulnerabilities		

Academic hours	Total 32 hours of e-learning.
Type of discipline	E-learning tools Cyber Range
EQF level	*2-4*
Preliminary requirements	Particularly good knowledge of English (at least B2 or C1) Have basic knowledge of programming (input)
Resources	*Moodle platform (or equivalent)* *Learning resources: reading resources, videos, materials, etc* *Cyber Range learning activities and cyber exercise scenarios.*

4.2.2 Occupational Profile 2 - PENETRATION TESTER

2.12 PENETRATION TESTER (IST).docx

PENETRATION TESTER
TRAINING AIM
The aim of the training is to introduce the learners to the role of Penetration Tester and increase their capacity to meet its main tasks. The educational material combines a good theoretical framework and innovative interactive e-learning methods, with emphasis to the use of a Cyber Range and the execution of specific cyber exercise scenarios. The training will be linked to a certification examination providing the learners with a formal recognition for the level of competencies they will have in the field of cybersecurity and the specific role of the Penetration Tester.

PENETRATION TESTER		
PROGRAMME OBJECTIVES		
By the end of this course, learners will acquire or develop specific knowledge, skills and attitudes which will allow them to assess the effectiveness of security controls, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors. The main competences of the course will unfold according to the revised ENISA Occupational Profile of the Penetrations Tester, as introduced within the framework of the REWIRE project (WP2) Learners will be able to plan, design, implement, and execute penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures. They will also be able to identify vulnerabilities or failures in technical and organizational controls that affect the confidentiality, integrity, and availability of ICT products (e.g., systems, hardware, software, and services).		
Knowledge	**Skills**	**Attitudes**
• Understand cybersecurity attack vectors • Know IT/OT appliances, operating systems, and computer networks • Aware of penetration testing tools, techniques, and methodologies • Label of security vulnerabilities and threats • List of best practices on cybersecurity	• Develop codes, scripts, and programmes • Identify systems weaknesses and security risks • Use penetration testing tools effectively • Evaluate and adapt / customise penetration testing tools and techniques • Communicate and report effectively	• Adopt conduct ethical hacking • Value teamwork and collaboration • Willing to learn and share expertise

Academic hours	*Total 32 hours of e-learning.*
Type of discipline	*E-learning tools* *Cyber Range*

EQF level	*2- 4*
Preliminary requirements	*Particularly good knowledge of English (at least B2 or C1)* *Have basic knowledge of programming*
Resources	*Moodle platform (or equivalent)* *Learning resources: reading resources, videos, materials, etc* *Cyber Range learning activities and cyber exercise scenarios.*

4.2.3 Occupational Profile 3 - CYBER THREAT INTELLIGENCE SPECIALIST

2.4 CYBER THREAT INTELLIGENCE SPECIALIST (EKT).docx

CYBER THREAT INTELLIGENCE SPECIALIST
TRAINING AIM
The aim of the training is to introduce the learners to the role of the Cyber Threat Intelligence Specialist and increase their capacity to meet its main tasks. The educational material combines a good theoretical framework and innovative interactive e-learning methods, with emphasis to the use of a Cyber Range and the execution of specific cyber exercise scenarios. The training will be linked to a certification examination providing the learners with a formal recognition for the level of competencies they will have in the field of cybersecurity and the specific role of the Cyber Threat Intelligence Specialist.

CYBER THREAT INTELLIGENCE SPECIALIST		
PROGRAMME OBJECTIVES		
By the end of this course, learners will be able to collect, process, analyze data and information to produce actionable intelligence reports and disseminate them to target stakeholders. The main competences of the course will unfold according to the revised ENISA Occupational Profile of the Cyber Threat Intelligence Specialist, as introduced within the framework of the REWIRE project (WP2) Learners will be able to manage cyber threat intelligence life cycle including cyber threat information collection, analysis and production of actionable intelligence and dissemination to security stakeholders and the CTI community, at a tactical, operational, and strategic level. They will also be in position to identify and monitor the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors and their trends, track threat actors' activities and observe how non-cyber events can influence cyber-related actions		
Knowledge	**Skills**	**Attitudes**
• Know of TTP frameworks • Aware of big data handling and analytics methods • Advanced knowledge of cybersecurity solutions, outputs, and integrity to comprehensive cybersecurity concept • Recall recent vulnerability disclosures, data breach incidents and geopolitical events impacting cyber risk • List advanced and persistent cyber threats and threat actors	• Work in a team and cooperate with different external partners setting intelligence process and operational environments • Collect, analyse, and correlate cyber threat information originating from multiple sources • Conduct technical analysis and reporting • Write and communicate intelligence reports to stakeholders	• Cares about new developments in the cybersecurity field • Is committed to provide detailed reports • Is prone to act preventively • Trusts their own skills and knowledges

• Understand intelligence disciplines, eco-system, and methodologies • Duplicate target methods and procedures	• Identify and model treats, actors, TTPs and campaigns • Determine appropriate targeting options and identify critical target elements	

Academic hours	*Total 32 hours of e-learning.*
Type of discipline	*E-learning tools* *Cyber Range*
EQF level	*2- 4*
Preliminary requirements	*Particularly good knowledge of English (at least B2 or C1)* *Have basic knowledge of programming*
Resources	*Moodle platform (or equivalent)* *Learning resources: reading resources, videos, materials, etc* *Cyber Range learning activities and cyber exercise scenarios.*

4.2.4 Occupational Profile 4 - CHIEF INFORMATION SECURITY OFFICER (CISO)

2.1 CHIEF INFORMATION SECURITY OFFICER (CISO) (LRQA).docx

CHIEF INFORMATION SECURITY OFFICER (CISO)
TRAINING AIM
The aim of the training is to introduce the learners to the role of the Chief Information Security Officer (CISO and increase their capacity to meet its main tasks. The educational material combines a good theoretical framework and innovative interactive e-learning methods, with emphasis to the use of a Cyber Range and the execution of specific cyber exercise scenarios. The training will be linked to a certification examination providing the learners with a formal recognition for the level of competencies they will have in the field of cybersecurity and the specific role of the Chief Information Security Officer (CISO).

CHIEF INFORMATION SECURITY OFFICER (CISO)		
PROGRAMME OBJECTIVES		
By the end of this course, learners will be able to collect, process, analyze data and information to produce actionable intelligence reports and disseminate them to target stakeholders. The main competences of the course will unfold according to the revised ENISA Occupational Profile of the Chief Information Security Officer (CISO), as introduced within the framework of the REWIRE project (WP2) Learners will be able to define, maintain and communicate the cybersecurity vision, strategy, policies, and procedures. They will also be able to manage the implementation of the cybersecurity policy across the organization and assure information exchange with external authorities and professional bodies.		
Knowledge	**Skills**	**Attitudes**
• Compare of cybersecurity and privacy standards, frameworks, policies, regulations, legislations, certifications, and best practices. • Know of security controls. • Classify risk management frameworks. • Understand incident management processes, frameworks, standards, best practices, and terminology. • Aware of existing and emerging technologies and their security characteristics.	• Analyse and implement cybersecurity risk management, design, and document the processes for risk analysis and management • Develop, champion, and lead the execution of a cybersecurity strategy • Communicate, coordinate, and cooperate with internal and external stakeholders • Define and apply maturity models for cybersecurity management, apply benchmarking and improvement/maturity models for security management	• Appreciate the value of a properly structured report • Seek proper collaboration and effective communication • Recognize the necessity of a well-established cybersecurity strategy • Trusts the input of others

	• Anticipate future cybersecurity threats, trends, needs and challenges in the Organization • Manage cybersecurity resources and related budget	

Academic hours	*Total 32 hours of e-learning.*
Type of discipline	*E-learning tools* *Cyber Range*
EQF level	*2- 4*
Preliminary requirements	*Particularly good knowledge of English (at least B2 or C1)* *Have basic knowledge of programming*
Resources	*Moodle platform (or equivalent)* *Learning resources: reading resources, videos, materials, etc* *Cyber Range learning activities and cyber exercise scenarios.*

5. BEST-PRACTICE GUIDANCE FOR THE CREATION OF STAKEHOLDER'S NETWORK ON CYBERSECURITY EDUCATION

5.1 Introduction

Building a stakeholder network for cybersecurity education is crucial to ensure that a wide range of perspectives are represented, and that the education program meets the needs of all stakeholders. These best practices can serve as a valuable resource for organizations looking to create their own stakeholder network for cybersecurity education, as it has been developed through collaboration between key stakeholders.

The main input of the proposed best practices is from the *CONCORDIA Governance model for a European Education Ecosystem for Cybersecurity*[7] and the experience of the partners involved in the creation of the CONCORDIA Governance model. By leveraging the experiences and best practices outlined in the CONCORDIA Governance model, organizations can create a stakeholder network that is not only effective but also sustainable in the long term, meeting the needs of all stakeholders involved.

5.2 Characteristics of a cybersecurity education network

The proposed model has several characteristics that are important for an effective governance approach for the Cybersecurity Education network. The characteristics include agility, inclusivity, trust, smart sovereignty, multimodality, flexibility, sustainability, impact focus, and methodological soundness.

1. Agility means that the governance approach should be efficient and forward-looking, anticipating problems before they arise. Inclusivity refers to the involvement of all stakeholders in the education ecosystem to anticipate potential risks and opportunities.
2. Trust-based governance involves sharing information and best practices to increase the body of knowledge that can be used as a basis for new policies.

[7] CONCORDIA Governance model for EEEC (https://www.concordia-h2020.eu/wp-content/uploads/2023/02/CONCORDIA_Governance_model_for_EEEC.pdf)

3. Smart sovereignty is needed to balance international cooperation with national autonomy, considering a multimodal approach covering national, regional, and EU level specificities.
4. Flexibility is important for accessing and participating in diverse groups' activities and interactions without being formally validated.
5. Sustainability in all aspects of the cybersecurity education network is important, including sustainable practices in education delivery, infrastructure, and resources, and sustainable funding mechanisms.
6. Impact focus involves placing a strong emphasis on measurement and monitoring to ensure that the cybersecurity education network is meeting its objectives effectively and efficiently.

Methodological soundness is important in the use of recognized monitoring, analytical, coordination, and co-creation tools to develop a complete set of tools from monitoring to coordination. By incorporating these characteristics into the governance approach, the cybersecurity education network can be managed more effectively, efficiently, and sustainably.

5.3 Best practices for the creation of the cybersecurity education network

Here are some best practices to follow when creating a stakeholder network for cybersecurity education:

1. Identify key stakeholders: Start by identifying the key stakeholders that are relevant to your cybersecurity education network. This may include IT (Information Technology) professionals, educators, industry experts, government officials, and community leaders, among others.

   Mapping the actors based on their level of influence and roles can provide a clearer understanding of the dynamics of the European cybersecurity education network. Stakeholders in the European cybersecurity education ecosystem can better understand the landscape and identify potential partners and collaborators. This can help promote collaboration and coordination and ultimately lead to the development of more effective and comprehensive cybersecurity education initiatives.

   The three categories of stakeholders based on their scope of operation can be defined as follows:

   - EU organizations, which operate at the level of the European Union or have an influence on a group of EU Member States.
   - National organizations, which operate at the level of individual EU Member States.
   - Local organizations, which operate at the city level or have an impact on a group of cities or regions within the same country.

   The roles are categorized as follows:

- Regulators, who are organizations that have a mission to regulate an area of activity for the public good. Examples include the European Commission, certification bodies, and national ministries.
- Aggregators, who are organizations that pull together a set of resources, both monetary and non-monetary, for the use of a community. Examples include ENISA, ECCC, and associations.
- Coordinators, who are organizations that are empowered to harmonize the usage of a set of resources to achieve specific education-related objectives.
- Influencers, who are organizations or individuals that have the capacity to affect the course of an action. This includes NGOs, think-tanks, and companies.
- Providers, who are organizations or individuals that offer education-related services to the market. Examples include universities, research organizations, training and solution providers, and corporates.
- Beneficiaries, who are organizations, groups, or individuals that benefit from the educational offer. This includes students, professionals, and small and large companies.

It should be noted that an actor within the cybersecurity education network may perform multiple roles and may have a level of influence on more than one level. For example, a university could be both a provider of educational services and an influencer within the ecosystem, and it could have a level of influence at both the national and EU levels.

2. Build relationships: Once you have identified the stakeholders, build relationships with them. This can be done through networking events, workshops, or other outreach activities. It is important to establish trust and demonstrate your commitment to their interests.
3. Develop a shared vision: Work with your stakeholders to develop a shared vision for your cybersecurity education program. This will help ensure that everyone is on the same page and working towards the same goals.
4. Encourage collaboration: Encourage collaboration between stakeholders. This can be done through workshops, focus groups, or other activities that bring people together to share their ideas and perspectives.

   To facilitate information exchange and accommodate the diverse interests of Cybersecurity education network actors, a proposed approach involves dividing discussions into two main categories: Policy talks and Operational talks.

   Policy talks would bring together representatives of Regulators, Aggregators, and Influencers at both EU and National levels, while Operational talks would bring together Coordinators, Providers, and Beneficiaries at both levels. These talks would occur at a predetermined frequency.

The outcomes of the Operational talks would inform the Political talks to aid in shaping EU policies for the benefit of the broader cybersecurity ecosystem. To ensure inclusivity of all interested actors, the proposed network suggests involving stakeholders from all role categories and levels. However, this approach would require a dedicated individual or organization per country to moderate the national section, translate input, and cluster different perspectives in preparation for the Policy and Operational talks.

5. Ensure diversity and inclusivity: Ensure that your stakeholder network is diverse and inclusive. This means actively seeking out and engaging stakeholders from a variety of backgrounds and perspectives and ensuring that everyone feels valued and heard.
6. Regular communication: Establish regular communication channels with your stakeholders. This can be done through email updates, newsletters, or social media groups. It is important to keep everyone informed and engaged throughout the process.
7. Evaluate and adjust: Regularly evaluate your stakeholder network and adjust your approach as needed. This will help ensure that your cybersecurity education program is meeting the needs of all stakeholders and achieving its goals.

Best practices for ensuring feedback on curricula information from stakeholders in a cybersecurity education network:

1. Establish a feedback mechanism: Create a formal process for stakeholders to provide feedback on the curricula information. This could be through a survey, focus groups, or other feedback mechanisms. Make sure to clearly communicate this process to stakeholders and encourage their participation.
2. Regularly review and update curricula information: Ensure that the curricula information is reviewed and updated regularly to reflect changes in the cybersecurity landscape. This can be done by forming a curriculum review committee consisting of subject matter experts and stakeholders.
3. Incorporate stakeholder feedback into curricula updates: Use the feedback received from stakeholders to update and improve the curricula information. Make sure to communicate these updates back to stakeholders to demonstrate that their feedback is valued and has been incorporated.
4. Engage stakeholders in curriculum development: Involve stakeholders in the development of new curricula information to ensure that it meets their needs and aligns with their priorities. This can be done through workshops, focus groups, or other collaborative activities.
5. Conduct regular evaluations: Conduct regular evaluations of the curricula information to ensure that it is effective and meeting the needs of stakeholders. This can be done through assessments, surveys, or other evaluation methods.

By following these best practices, it is possible to create a stakeholder network for cybersecurity education that is not only effective in providing feedback on curricula

information but also helps ensure that the curriculum information is up-to-date and meets the needs of stakeholders.

6. SUMMARY AND CONCLUSIONS

The REWIRE Curricula and Training Framework is a comprehensive guide that outlines the objectives, structure, total hours, and training methods to be used for the development of the trainings and training material for the selected ENISA Occupational Profiles; Cyber Incident Responder, Penetration Tester, Cyber Threat Intelligence Specialist, and Chief Information Security Officer (CISO). It is basically a roadmap for all the involved partners, ensuring that everyone involved in the training development will be on the same page and understands what is expected of them.

The Framework defines the training aims and learning objectives of the program, indicating what participants are expected to gain from completing the training. It also describes the structure of the program, including the number of modules and the topics that will be covered and the sequence in which they will be presented. The total hours of the training program are also specified, along with the time commitment required from participants. Additionally, the Framework indicates the training methods that were agreed to be used to deliver the training.

The Framework is open to revisions and adjustments that may arise during the creation of the training material and the feedback received during the pilots. A definitive version of it is expected to be delivered and accompany the final training material. This version will be an integral part of the final training, to be used by the trainers and trainees, ensuring that they are aware of the type and the requirements of the training, as well as of the expected learning outcomes linked to it.

The document also describes the multi-criteria selection methodology, which was developed and used to select the occupational profiles and it includes a best-practice guidance for creating a stakeholder's network on cybersecurity education. Both are vital resources to be capitalized on within the project and be used as good practices for future projects within and without the cybersecurity field.