REWIRE
CYBERSECURITY SKILLS ALLIANCE

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

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R3.3.1. Cybersecurity Skills Framework

Title	R3.3.1. Cybersecurity Skills Framework
Document description	The report presents the REWIRE Cybersecurity Skills Framework, drawing on ENISA skills framework version 2 (draft version 0.5), considering the classification of European Skills, Competences, Qualifications and Occupations (ESCO) and other existing competence frameworks.
Nature	Public
Task	T3.3.1 Cybersecurity Skills Framework
Status	Final
WP	WP3
Lead Partner	MRU
Partners Involved	BUT, KTH, EKT, MUNI, EUC, CCC. TUC, ReadLab, ApiroPlus, Hellenic Lloyd's, URL, NRD CS, IMT
Date	25/10/2022

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CONTENTS

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

LIST OF ABBREVIATIONS AND ACRONYMS

Table 1: List of abbreviations and acronyms

Abbreviation	Explanation/ Definition
ECSF	European Cybersecurity Skills Framework
EC	European Commission
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
EU	European Union
ICT	Information and Communication Technologies
ASD	The Australian Signals Directorate
CEN	European Committee for Standardization
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology of the U.S. Department of Commerce

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

LIST OF TABLES

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

EXECUTIVE SUMMARY

The REWIRE project team has worked extensively on the 12 profiles contained within version 0.5 of the ECSF[i] proposed by ENISA and the relevant ad-hoc working group and has provided an enhanced cybersecurity skills framework covering gaps in competences, skills and knowledge identified while reviewing other similar documents.

This work has included:

- Analysis of existing practices by the ICT-03 pilots (CONCORDIA[ii], ECHO[iii], CyberSec4Europe[iv], SPARTA[v]) respective training and education work-packages.
- A review of all the information within the profiles.
- An examination of existing information from other national and international cybersecurity skills frameworks;
- A correlation between the profiles to identify any gaps.
- A re-phrasing / writing of the tasks so that specific action words are used and the same language is shared for all tasks.
- A correlation of each task to the needed knowledge, skills and competences and
- A review of the ESCO skills and knowledge taxonomies and contents so that further skills/knowledge (not digital ones) could be identified and added.

The results of the above efforts have been recomposed and are contained in the REWIRE Cybersecurity Skills Framework which is compared to ENISA's proposal for ECSF v0.5.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

INTRODUCTION

Purpose and objective

This document is produced in the context of WP3, "Design of the European Cybersecurity Blueprint". It presents the results of task 3.3, "Development of the European Cybersecurity Skills Framework".

The task has two aims, according to the description of the project, that describe the objective of the document:

1. *Analyze the existing information on Competences, Qualifications and Occupations and existing cybersecurity skills frameworks.*
2. *Revise and create occupational profiles and the corresponding skills needs, drawing on the classification of European Skills, Competences, Qualifications and Occupations (ESCO) and other existing competence frameworks.*

The results are consolidated under one Cybersecurity Skills Framework.

Scope

This document provides an analysis and extension of the ENISA's cybersecurity skills framework v2, that has been under the review while the report was prepared. It analyzes and extends the skills proposed by ENISA with content from ESCO and other provenance, to provide more extensive job profiles.

Structure of the document

The first chapter of the document describes, in short, the rationale behind the need of ECSF, the process of its development, the structure of the document and the definitions included. Furthermore, it describes the methodology to identify role profiles and then the content of these role profiles used by the REWIRE team.

The second chapter of the report consolidates the results of the systematic review into separate lists of competences, skills, and knowledge. It also proposes the definitions to the action verbs on tasks, the structure and hierarchy of the role profiles.

In the third chapter of the report, the competences, skills, and knowledge are combined with the tasks attached to a particular role profile and compared to those proposed by ENISA.

Readers of the document

The readers of the document include:

- Training providers, describing the competences and skills that their training programs will deliver to students based on the industry's necessities.
- Human resources managers, to:
    - provide clear role profiles that indicate to prospective candidates the set of competences and skills needed.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

  - Evaluate applicants based on the match between skills and evidence provided by a candidate.
  - Propose career evolutions to employees, that are supported by the relevant training programs.
- Cybersecurity professionals, to develop their career objectives and paths, and evaluate both job offers and training programs in relation to their needs.

Lifecycle of the document

This document is the first version, focusing on existing frameworks and contributions from the Pilot projects.

ENISA has been working on the second release of their skills framework while the report was prepared. Due to the timeframe of the release, this document focused on contribution to the enhancement of the ENISA skills' framework v2 that can be incorporated in the future release. REWIRE profiles were submitted to ENISA for consideration in June 2022.

This document references the vision of the REWIRE project at M23. Two yearly updates are planned at M36 and M48 within R3.6.1.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

1. DEVELOPING CYBERSECURITY SKILLS FRAMEWORK

1.1. REVIEW OF EXISTING ECSF

1.1.1. ENISA and development of the ECSF

The cybersecurity workforce shortage and skills gaps are a major concern for both economic development and national security, especially in the rapid digitization of the global economy[vi].

Europe lags behind in the development of a comprehensive approach to define a set of roles and skills relevant to the cybersecurity field, as described in the ENISA Report "Cybersecurity Skills Development in the EU" (ENISA, 2020). Though cybersecurity is a worldwide challenge affecting all countries, there are many differences in the ways it is approached by each state. For this reason, existing national cybersecurity frameworks may be incompatible or in general not targeted to the European needs, laws and regulations[vii].

The development of a European Cybersecurity Skills Framework (hereinafter ECSF) that would consider the needs of the EU and each one of its Member States was considered by ENISA an essential step towards Europe's digital future[viii].

The ECSF aims to create a common understanding of the roles, competences, skills, and knowledge used by and for individuals, employers and training providers across the EU Member States, in order to address the cybersecurity skills shortage. Additionally, it helps to further facilitate cybersecurity-related skills recognition and support the design of cybersecurity-related training programs for skills and career development. Consequently, the European Cybersecurity Skills Framework will boost employment and employability in cybersecurity-related positions[ix].

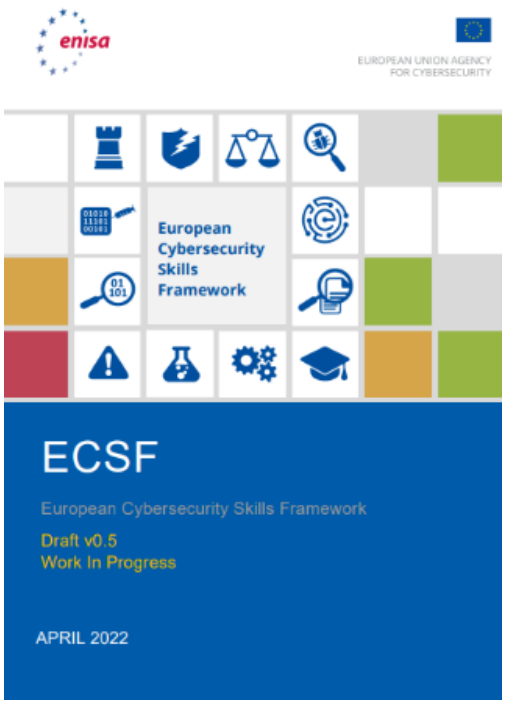
The ECSF resulted from the joint work of ENISA and a relevant Ad Hoc Working Group on the ECSF. The Group was formed in July 2020, following an ENISA public call for the creation of a multi-disciplinary group of experts with the task to promote harmonization in the ecosystem of cybersecurity education, training, and workforce development and develop a common European dialect for cybersecurity skills.

The ED DECISION No 55/2020 of the Executive Director of 5 November 2020 has established the ad-hoc group and the lists of selected candidates for membership. The Ad Hoc Working

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Group on the European Cybersecurity Skills Framework began working in December 2020 and analysed - in a methodological manner - other frameworks available at national, European, and international level, and conducted a market analysis[x].

On April 5, 2022, a consolidated draft version of the ECSF was presented to the public through a webinar, revealing the framework structure and benefits, along with various use cases[xi].



1.1.2. The 0.5. Draft version of the European Cybersecurity Skills Framework

1.1.2.1. Profiles

The 0.5. Draft version of the ECSF contains the following 12 profiles:

1. Chief information security officer (CISO)
2. Cyber incident responder
3. Cyber legal, policy & compliance officer
4. Cyber threat intelligence specialist
5. Cybersecurity architect
6. Cybersecurity auditor
7. Cybersecurity educator
8. Cybersecurity implementer
9. Cybersecurity researcher
10. Cybersecurity risk manager
11. Digital forensics investigator
12. Penetration tester

The document does not contain the methodology based on which the profiles have been constructed but based on the information provided during the related webinar, there will be a separate document that will contain such information[xii].

Each profile comprises of the following components:

- Title.
- Alternative title(s) (lists titles under the same profile).
- Summary statement (indicates the main purpose of the profile).
- Mission (describes the rationale of the profile).

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

- Deliverable(s) (illuminate the profiles and explains relevance including the perspective from a non-cybersecurity/ict point of view).
- Main task(s) (provides a list of typical tasks performed by the profile).
- Key skill(s) (provides a list of abilities to perform work functions and duties by the profile).
- -competences (from e-CF).
  key knowledge (provides a list of essential knowledge required to perform work functions and duties by the profile). Key knowledge is dividing into three groups depending on the level: basic understanding of, knowledge of, advanced knowledge of).

1.1.2.2. Definitions

A skills framework relies on an exhaustive classification of roles, functions, and actual tasks.

The role definitions provide the complete scope of "what are specialists doing in the organization, unit or role":

- *Skill*: the ability to use know-how and expertise to complete tasks and solve problems[xiii]. Skill is often defined as an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cybersecurity rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual[xiv]. The ability to carry out managerial or technical tasks[xv] .
- *Task*: is a specific defined piece of work that, combined with other identified Tasks, composes the work in a specific specialty area or work role[xvi].
- *Knowledge*: Body of facts, principles, theories and practices that is related to a field of work or study. An employee needs to know the relevant selection of these to successfully perform in their job[xvii]. Knowledge is a body of information applied directly to the performance of a function[xviii]. Represents the "set of know-what" (e.g. programming languages, design tools…) and can be described by operational descriptions[xix].
- *e-competence*: IT Professional competence as required and performed in IT work context[xx].
- *Role profile*: the function of the Professional Role Profiles is to offer users structure and clarity for designing or identifying and clustering the multitude of activities that are essential to support the digital strategy of an organization. They are less detailed and less specific than job descriptions and offer a simple but flexible start point[xxi].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

1.2. THE REWIRE EFFORTS

1.2.1. Methodology to identify Role Profiles

The 0.5. draft of the ECSF includes already 12 different profiles as mentioned above.

A Cybersecurity Skills Framework should comprise of as many role profiles as possible, to be able to support the market and its needs effectively.

For the identification of the role profiles, the following methodology was created and followed by the REWIRE project.

a. Identification of existing cybersecurity skills frameworks:
   i. The Cybersecurity Skills Framework for ICT of Singapore, or the Skills Framework for infocomm technology, with a focus on roles on the Cyber Security and infrastructure tracks[xxii].
   ii. ASD Cyber skills framework of Australia defines the roles, capabilities and skills proficiencies that are essential to cyber missions, and that can be used in both the security and offensive contexts[xxiii]. The ASD Cyber Skills Framework v.2.0 introduces additional elements, as follows: role definitions and expectations, digital Career Pathways, learning and Development pathways, national Initiative for Cybersecurity Education (NICE) work roles, Australian Defence Force (ADF) professional framework[xxiv].
   iii. The European ICT Professional Role Profiles[xxv]. European Committee for Standardization (CEN) provides a generic set of typical roles performed by IT Professionals in any organisation, covering the full range of ICT business processes, using the European e-Competence Framework (e-CF) as the basis for competence identification, illuminating and structuring each ICT Professional Profile with a number of components including work outcomes or "Deliverables"[xxvi].
   iv. The National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) developed by National Institute of Standards and Technology of the U.S. Department of Commerce (NIST)[xxvii].
   v. The ECHO Cyberskills Framework[xxviii], which provides a better definition of the knowledge and skill gaps in the healthcare, transport, and energy industries as well as for the development of cybersecurity education and training programs that address those gaps. Focusing on hospitals, energy companies, ship crews, and outsourced (third-party) Security Operation Centres (SOC), the project identified the following 11 cybersecurity professional roles: Cyber Defense Incident Responder, Cyber Defense Infrastructure Support Specialist, Cyber Instructor, Cyber Operator, Information Systems Security Developer, Information Systems Security Manager, Privacy Officer/Privacy Compliance

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Manager, Security Architect, Security Control Assessor, System Security Analyst, Communications Security (COMSEC) Manager.

vi. The global skills and competence framework for the digital world developed by the British SFIA Foundation[xxix]. The SFIA Framework contains roles, their levels, and the skills for each role.

b. Job analyzer

The above existing cybersecurity skills frameworks provide a very useful course of information regarding the following: a) Identified Roles and b) The skills, knowledge and competences identified for each one of the identified roles.

For a skills framework to be as effective and suitable as possible, there should also be a way that new roles are identified and added. This information could come from the market itself – the current job ads. The same channel can be also used for the validation of the skills, knowledge and competences identified and associated by the market per Role.

Specifically, a first analysis of the ads of the Job analyzer, provided:

- 20 Roles (8 additional to those proposed by ENISA in the ECSF draft v.05)
- For each of the identified roles, various titles appear in the ads without them following a specific rule in every case.
- The role of the Cybersecurity Impelementer appears to have the most alternative titles. From the examined ads (358), 178 correspond to the role of the Cybersecurity Implementer. The identified alternative titles are 20 including Cyber security Engineer, Cyber security Specialist and others.

The work on the job analyzer will continue and in future deliverables will include information on the validation of the skills and knowledge of the roles as well as the level identified for each role.

c. Other sources, like:

i. Job profiles, their analysis[xxx] and an interactive career map tool[xxxi] developed by Security Talent, an initiative of Security Delta (HSD), a Dutch security cluster.

ii. Cyber Secrity Career pathway developed by the Cyberseek, which shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skillsets associated with each role[xxxii].

iii. Cyber Career Pathways Tool that depicts the Cyber Workforce according to five distinct skill communities, highlights core attributes among each of the 52 work roles and offers actionable insights for employers, professionals, and those considering a career in Cyber. It offers an interactive way to explore work roles within the NICE Framework[xxxiii].

iv. The occupations classification platform of ESCO, which was developed by the DG Employment, Social Affairs and Inclusion of the European Commission in collaboration with stakeholders and with the European Centre for the

Development of Vocational Training (Cedefop). The ESCO platform[xxxiv] contains an analysis of occupations, a basic hierarchy and an analysis of skills and competences per occupation.

1.2.2. Methodology to define the contents of the Role Profiles

For each one of 12 ENISA roles profiles, the same, similar, or close matches were identified (if they exist) to the frameworks and other sources identified above (Section 1.2.1.). Each one of the ENISA roles profiles was enhanced by the tasks, knowledge, skills, and competences that were missing. Possible alternative titles were added as well. To ensure the use of the same language for the same knowledge, all profiles were deconstructed, and one list of tasks (Section 2.1.4), skills (Section 2.2) and knowledge (Section 2.3) was established. It was revised linguistically and content-wise to ensure that the same language was used in all the job descriptions. Competences, skills, and knowledge were combined with the tasks attached to a particular role profile (see part 3).

Further analysis was conducted to correlate the tasks/skills/knowledge and e-competences. The purpose of the further analysis was to identify gaps in certain profiles, where the tasks are unaccompanied by knowledge, skills or competences, or cases where a logical transition could not be performed between the different profiles.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

2. TASKS, SKILLS, KNOWLEDGE, COMPETENCES

2.1. TASKS

2.1.1. Action verbs on tasks

Advise: to give someone useful information, or to tell them what you think they should do[xxxv]
Analyze: to study or examine something in detail in order to discover or understand more about it[xxxvi]
Assess: to judge or decide the amount, value, quality, or importance of something[xxxvii]
Assist: to take action to help someone or support something[xxxviii]
Audit: systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled[xxxix].
Communicate: to share information with others by speaking, writing, or using other signals[xl]
Design: to decide how something will look, work, etc., by drawing plans, making computer models, etc.[xli]
Develop: to (cause something to) grow or change into a more advanced, larger, or stronger form[xlii]
Document: to record the details of an event, a process, etc.[xliii]
Evaluate: to judge or calculate the quality, importance, amount, or value of something[xliv]
Identify: to recognize a problem, need, fact, etc. and to show that it exists[xlv]
Implement: to put a plan/policy/measure into action[xlvi]
Manage: coordinated activities to direct and control an organization[1][xlvii]
Monitor: determining the status of a system, a process, a product, a service, or an activity
Support: to agree with and give encouragement to someone or something because you want him, her, or it to succeed[xlviii]
Test: determination according to requirements for a specific intended use or application. Note 1 to entry: If the result of a test shows conformity, it can be used for purposes of validation[xlix].
Train: to prepare someone or yourself for a job, activity, or sport, by learning skills and/or by mental or physical exercise[l]
Analysis of text based on Text and word count analyzer | Lexicool.

[1] Management can include establishing policies and objectives, and processes to achieve these objectives

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

2.1.2. Structure and hierarchy of Role Profiles

One of the possible use cases of the Role Profiles is the career map. Specifically, it is desired that professionals (interested in a career in Cybersecurity – re-skilling or up – skilling) would have the ability to receive information:

- What each role entails.
- Which are the minimum skills / knowledge and e-competences that a person should have to implement the role effectively.
- What is the difference between a persons' existing knowledge and skills to those required (at a minimum) by the role profile.
- What knowledge, skills and e-competences are needed to transverse between one role and another.

To be able to derive this information, it is necessary that a hierarchical structure between the role profiles is created.

It should be noted that the 12 role profiles proposed by ENISA and the ad-hoc working group on Cybersecurity Skills, do not incorporate the element of hierarchy. On the other hand, the profiles themselves seem to cover various levels of expertise and maturity of the job role.

For example, the mission of the Cybersecurity implementer (Profile 2.8) is the following: "Provides cybersecurity-related technical development, integration, testing, implementation, operation, maintenance, monitoring and support of cybersecurity solutions, ensures adherence to specifications and conformance requirements, assures sound performance and resolves technical issues required in the organisation's cybersecurity-related solutions (systems, assets, software, controls and services), infrastructures and products."

The person that will implement this role would be asked to implement a range of activities that would cover from support to implementation, maintenance and operation. When making the correlation to the e-cf levels, the role seems to cover the first three levels, depending on the size of the organization and the relevant implementations and groups, the experience of the person, the complexity of the business environment etc.

Level 1: **Has the ability to apply knowledge and skills to solve straight forward problems: responsible for own actions; operating in a stable environment**.

Influence: implements Instructions.
Complexity: structured – predictable.
Autonomy: demonstrates limited independence where contexts are generally stable with few variable factors.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Behaviour: applying, adapting, developing, deploying, maintaining, repairing, finding basic - simple solutions.

Level 2: **Operates with capability and independence in specified boundaries and may supervise other in this environment; conceptual and abstract model building using creative thinking; uses theoretical knowledge and practical skills to solve complex problems within a predictable and sometimes unpredictable context.**

Influence: applies and adapts.
Complexity: structured – predictable.
Autonomy: works under general guidance in an environment where unpredictable change occurs. Independently resolves interactive issues which arise from project activities.
Behaviour: designing, managing, surveying, monitoring, evaluating, improving, finding non-standard solutions, scheduling, organizing, integrating, finding standard solutions, interacting, communicating, working in team.

Level 3: **Respective for innovative methods and use of initiative in specific technical or business areas; providing leadership and taking responsibility for team performances and development in unpredictable environments.**

Influence: consults.
Complexity: structured – unpredictable.
Autonomy: works independently to resolve interactive problems and addresses complex issues. Has a positive effect on team performance.
Behaviour: planning, making decisions, supervising, building teams, forming people, reviewing performances, finding creative solutions by application of specific technical or business knowledge / skills.

The fact that this role can range between different levels is reflected also in the results of the analysis of the Job offerings (Job analyzer) and in some of the other Cybersecurity Skills Frameworks. Specifically, in the analysis of the job offerings by the Job Analyzer, profiles are identified with prefixes such as Senior, Junior, Associate, Tier 1, Assistant, etc.

To facilitate the market needs, it is recommended that the profiles are split into three categories / levels: ***Junior, Middle, Senior***; for each level the relevant skills, knowledge, e-competences and other expertise are identified and aligned.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

2.1.3. Hierarchy of the roles

The following tables depict the e-competences that have been identified by the project team as required (M=Mandatory) and Optional (O), and their corresponding level as defined by the e-cf (e-competence framework)[2].

CHIEF INFORMATION SECURITY OFFICER (CISO)

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Plan	A.1. IS and Business Strategy Alignment					M
Plan	A.2. Service Level Management				M	
Plan	A.5. Architecture Design			M		
Plan	A.6. Application Design	O				
Build	B.3. Testing	O				
Build	B.5. Documentation Production			M		
Run	C.4. Problem Management				M	
Run	C.5. Systems Management	O				
Enable	D.1. Information Security Strategy Development					M
Manage	E.3. Risk Management				M	
Manage	E.7. Business Change Management				M	
Manage	E.8. Information Security Management				M	
Manage	E.9. Information Systems Governance				M	

CYBER INCIDENT RESPONDER

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Plan	A.7. Technology Trend Monitoring				M	
Plan	A.9. Innovating				M	
Enable	D.1. Information Security Strategy Development				M	
Enable	D.10. Information and Knowledge Management				M	
Manage	E.8. Information Security Management				M	

CYBER LEGAL, POLICY & COMPLIANCE OFFICER

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Plan	A.1. IS and Business Strategy Alignment				M	

[2] CWA 16458-1:2018 European ICT Professional Role Profiles – Part 1: 30 ICT Profiles, CWA 16458-3:2018 European ICT Professional Role Profiles – Part 3: Methodology, DIN EN 16234-1:2020-02 e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors - Part 1: Framework; German version EN 16234-1:2019

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Run	C.4. Problem Management		M			
Enable	D.1. Information Security Strategy Development				M	
Enable	D.3. Education and Training Provision		M			
Enable	D.5. Sales Development			M		
Enable	D.10. Information and Knowledge Management				M	
Manage	E.3. Risk Management			M		
Manage	E.4. Relationship Management			M		
Manage	E.8. Information Security Management			M		
Manage	E.9. Information Systems Governance				M	

CYBER THREAT INTELLIGENCE SPECIALIST

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Plan	A.2. Service Level Management				M	
Plan	A.7. Technology Trend Monitoring				M	
Build	B.5. Documentation Production			M		
Build	B.6. ICT Systems Engineering			M		
Enable	D.1. Information Security Strategy Development				M	
Enable	D.7. Data Science and Analytics			M		
Enable	D.10. Information and Knowledge Management				M	
Manage	E.4. Relationship Management				M	
Manage	E.8. Information Security Management				M	
Manage	E.9. Information Systems Governance				M	

CYBERSECURITY ARCHITECT

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Plan	A.1. IS and Business Strategy Alignment					M
Plan	A.3. Business Plan Development				M	
Plan	A.5. Architecture Design					M
Plan	A.6. Application Design	M				
Plan	A.7. Technology Trend Monitoring				M	
Build	B.1. Application Development			M		

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Build	B.2. Component Integration				M	
Build	B.3. Testing			M		
Build	B.4. Solution Deployment			M		
Build	B.5. Documentation Production			M		
Build	B.6. ICT Systems Engineering				M	
Run	C.4. Problem Management			M		
Enable	D.1. Information Security Strategy Development				M	

CYBERSECURITY AUDITOR

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Plan	A.4. Product / Service Planning				M	
Build	B.5. Documentation Production			M		
Enable	D.10. Information and Knowledge Management				M	
Manage	E.3. Risk Management				M	
Manage	E.4. Relationship Management			M		
Manage	E.6. ICT Quality Management				M	
Manage	E.8. Information Security Management				M	

CYBERSECURITY EDUCATOR

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Plan	A.7. Technology Trend Monitoring				M	
Build	B.5. Documentation Production		M			
Enable	D.3. Education and Training Provision			M		
Enable	D.9. Personnel Development			M		
Manage	E.3. Risk Management			M		
Manage	E.8. Information Security Management				M	

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CYBERSECURITY IMPLEMENTER

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Plan	A.5. Architecture Design			M		
Plan	A.7. Technology Trend Monitoring			M		
Build	B.2. Component Integration			M		
Build	B.3. Testing			M		
Build	B.4. Solution Deployment			M		
Build	B.5. Documentation Production		M			
Build	B.6. ICT Systems Engineering				M	
Run	C.1. User Support		M			
Run	C.4. Problem Management			M		
Run	C.5. Systems Management			M		
Enable	D.1. Information Security Strategy Development				M	
Manage	E.3. Risk Management		M			
Manage	E.8. Information Security Management			M		

CYBERSECURITY RESEARCHER

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Plan	A.6. Application Design		M			
Plan	A.7. Technology Trend Monitoring					M
Plan	A.9. Innovating					M
Build	B.1. Application Development		M			
Build	B.3. Testing		M			
Run	C.4. Problem Management			M		
Enable	D.4. Purchasing		M			
Enable	D.7. Data Science and Analytics				M	
Enable	D.10. Information and Knowledge Management			M		
Manage	E.3. Risk Management		M			

CYBERSECURITY RISK MANAGER

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Build	B.2. Component Integration				M	
Build	B.5. Documentation Production		M			
Enable	D.1. Information Security Strategy Development					M
Enable	D.7. Data Science and Analytics				M	

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Enable	D.10. Information and Knowledge Management				M	
Manage	E.3. Risk Management				M	
Manage	E.8. Information Security Management			M		
Manage	E.9. Information Systems Governance				M	

DIGITAL FORENSICS INVESTIGATOR

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Plan	A.7. Technology Trend Monitoring			M		
Build	B.3. Testing				M	
Build	B.5. Documentation Production			M		
Enable	D.10. Information and Knowledge Management				M	
Manage	E.3. Risk Management			M		
Manage	E.8. Information Security Management			M		

PENETRATION TESTER

Dimension 1	Dimension 2	e-1	e-2	e-3	e-4	e-5
Build	B.2. Component Integration				M	
Build	B.3. Testing				M	
Build	B.4. Solution Deployment		M			
Build	B.5. Documentation Production			M		
Manage	E.3. Risk Management				M	

2.1.4. List of tasks

Once the gaps were identified, to ensure the use of the same language for the same task, all profiles were deconstructed, and one list of tasks (see the table below) was established. It was revised linguistically and content-wise to ensure that the same language was used in all the role profiles.

Table 2: List of tasks

Task Description
Act as a key contact point to handle queries and complaints regarding data processing;
Adapt third party training material to support individual competence development in line with organizational needs.
Advise and **support** internal stakeholders on subjects related to penetration testing.
Advise different functions internally on cybersecurity risks, methodologies, tools, updates, threat scenarios etc.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Task Description
Advise internal stakeholders on how to secure and preserve digital evidence and the relevant constraints and processes.
Advise on cybersecurity skills certification schemes and certificates.
Advise on mitigation plans at the tactical, operational and strategic level.
Advise on threat modelling, risk mitigation and cyber threat hunting based on intelligence data
Advise on, **design**, **develop** and **update** documents due to the introduction of existing, new or revised laws, regulations, executive orders, policies, standards, or procedures.
Advise the top Management on the economics of cybersecurity.
Advise top management on risk levels and security posture.
Advise, support and **coordinate** with internal stakeholders on subjects related to cybersecurity and privacy compliance requirements.
Advocate organization's official position in legal and legislative proceedings.
Analyse and **evaluate** the organisation's architecture in relation to cybersecurity.
Analyze hardware components.
Analyze malicious code for evidence of ATT&CK patterns and provenance.
Analyze, **assess** and **evaluate** the effectiveness of cybersecurity related policies, processes, procedures, standards or practices in relation to relevant applicable laws and regulations.
Analyze, **collect** and **evaluate** evidence of possible security events and incidents.
Assess cybersecurity risks and **advise** on appropriate risk treatment options in alignment with the business strategy and objectives.
Assess the implemented architecture against cybersecurity requirements and goals, aiming at the maintenance of an appropriate level of security.
Assist in the **Design**, **development**, **implementation** and **management of** disaster recovery, business continuity and incident response policies, procedures, plans, standards and guidelines. m
Assist in the **Design**, **development**, **implementation** and **management of Risk Management** within the organization. Have ownership and overview of the Risk Management process.
Collaborate and **communicate** with stakeholders to identify and/or develop appropriate solutions technology.
Collaborate with and **advise** other teams and colleagues, on the related subjects.
Collaborate with the IT/OT personnel on cybersecurity-related actions.
Collect, **analyze**, **produce** and **communicate** actionable intelligence as needed.
Communicate cybersecurity related risks, issues, updates, processes and actions internally as needed.
Communicate the high-level security architecture design to stakeholders.
Communicate with internal and external stakeholders to ensure appropriate resources are deployed internally or externally to support the risk management process.
Conduct (wholly or partially) privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures.
Conduct experiments and **develop** proof of concept(s), pilot(s) and prototypes for cybersecurity solution.
Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.
Conduct research, innovation and development work in cybersecurity-related topics.
Cooperate and **communicate** with authorities and professional groups as needed.
Coordinate and **advise** enterprise-wide cyber defense technicians on resolution of cyber defense incidents
Coordinate incident response activities.
Coordinate with stakeholders to share and consume intelligence on relevant cyber threats
Define (for each individual audit) the cybersecurity audit scope (including the target environment), objectives and criteria.
Design and **advise** on a secure architecture aligned to the organisation's strategy and the security and privacy requirements.

Task Description
Design and **implement** changes (adpations) to the organisation's architecture in response to emerging cybersecurity related threats.
Design and **implement** security reviews and assessments, **support** the relevant certification processes and **respond** to resulting open issues.
Design and **manage** Cybersecurity Audit Policies, Procedures, Standards and guidelines.
Design and **manage** Cybersecurity Policies & Procedures in alignment with the business strategy to support the organizational objectives (Fully or partially).
Design and **manage** data management and sharing procedures and policies, taking into consideration relevant legal, regulatory, industry and company constraints
Design and **Manage** intelligence development process in accordance to relevant requirements
Design and **manage** the organisation's cyber threat intelligence strategy
Design methodologies and practices used for cybersecurity audits.
Design plans and procedures to manage threat intelligence.
Design, **develop** and **manage** the organization's cybersecurity risk management strategy in alignment with the business strategy to support the organizational objectives.
Design, **develop**, **implement** and **manage** cybersecurity policies, processes, procedures, standards, plans, guidelines and frameworks (including roles and responsibilities) in alignment with the business strategy to support the organizational objectives.
Design, **develop**, **implement** and **manage** cybersecurity risk management policies, processes, procedures, standards, guidelines and frameworks (including roles and responsibilities).
Design, **develop**, **implement** and **manage** digital forensics investigation policies, processes, procedures, standards, guidelines and plans.
Design, **develop**, **implement** and **manage** test plans and procedures for penetration testing (including result analysis and reporting).
Design, develop, implement, manage and continually **improve** the information security management system.
Design, **develop**, **update** and **deliver** cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need.
Design, **document** and **communicate** cyber defense techniques, guidance, and reports on incident findings as needed.
Design, **document** and **implement** cyber incident management policies, procedures and plans
Design, **implement, manage, review and update** cybersecurity audit plan(s) containing the needed components (frameworks, standards, methodologies, procedures, tests, objectives etc) in alignment with the risk profile(s).
Determine appropriate targeting options and identify critical target elements.
Develop innovative cybersecurity-related solutions (in total or partially).
Document and **communicate** (as needed) architectural specifications, requirements and other related information.
Document and **communicate** as needed after action reviews, lead the lessons learned sessions etc.
Document and **communicate** as needed based on threat intelligence data.
Document and **communicate** effectively to Top Management as needed on cybersecurity incidents, risks, findings.
Document and communicate opportunities for improvement as a result of assessments, audits and tests.
Document and **communicate** penetration testing results to stakeholders as needed. **Classify** findings, **propose** mitigation actions and re-**test** as needed**.**
Document and **communicate** scientific works and research and development results.
Document and **communicate** the information, evidence, opportunities for improvement, deviations, other information and conclusions of the assessment, audits and tests.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Task Description
Document and **communicate** to Top Management as needed on cybersecurity incidents, risks, findings.
Document information and results related to the security of systems, services and products. **Communicate** as needed.
Document the information and results of the Risk Management process and individual activities.
Document, **report** and **communicate** (for information and approval where needed) the cybersecurity vision, strategy and risks (risk appetite, residual risk etc) to top management.
Document, **report** and **communicate** digital forensic analysis findings and results in a systematic, professional and deterministic manner.
Educate, **monitor** and **assess** the awareness of organization members and external parties on cybersecurity and privacy issues as needed.
Educate, monitor and assess the awareness of organization members as needed.
Enforce and **advocate** organisation's data privacy and protection program
Establish relationships, **collaborate** and **communicate** with stakeholders as needed (including cybersecurity-related authorities and communities).
Evaluate the impact of cybersecurity solutions on the design and performance of the organisation's architecture
Identify and **analyze** the threat landscape (including attackers' profiles and estimation of attacks' potential).
Identify and **implement** suitable approaches for education, training and awareness-raising based on needs.
Identify and **interpret** patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.
Identify and **resolve** conflicts between relevant applicable laws and regulations and cybersecurity policies, processes, procedures, standards or practices.
Identify attack vectors, **uncover** and **demonstrate** exploitation of technical cybersecurity vulnerabilities.
Identify cross-sectoral cybersecurity achievements and **apply** them in a different context or propose innovative approaches and solutions
Identify, **analyse** and **assess** cybersecurity technologies, solutions, developments and processes.
Identify, **analyse** and **assess** technical and organisational cybersecurity vulnerabilities.
Identify, analyze and **assess** cybersecurity-related threats and vulnerabilities.
Identify, **conseptualize** and **generate** research and innovation ideas, to advance the current state-of-the-art in cybersecurity-related topics.
Identify, **monitor** and **assess** the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors, the model threats, actors and campaigns
Identify, **plan**, **implement**, **apply** and **manage** patches to products to address technical vulnerabilities. **Respond** to issues by implementing required actions as needed.
Identify, **recover**, **extract**, **document** and **analyse** digital evidence.
Identify, **select** and **apply** frameworks, methods, standards, tools and protocols (including building and testing proof of concept(s)) to support projects.
Identify, **select** and **customise** (as needed) forensics testing, analysing and reporting techniques
Identify, **select**, **develop** and **customize** appropriate penetration testing techniques.
Implement cybersecurity procedures and controls.
Implement, **customize**, **operate**, **maintain**, **upgrade** and **test** cybersecurity products.
Inspect environments for evidence of unauthorised and unlawful actions.
Install, **customize**, **operate**, **maintain** and **upgrade testing tools (platforms, harware and software).**
Integrate cybersecurity solutions and **ensure** their sound operation.
Lead or **participate** in the innovation processes and projects including project management and budgeting.
Maintain and **protect** the integrity of cybersecurity audit records.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Task Description
Manage cybersecurity audit activities.
Manage legal aspects of information security responsibilities and third-party relations.
Manage the development, integration and maintenance of cybersecurity architecture.
Monitor advancement in cybersecurity and the internal and external context.
Monitor external data sources (e.g., Computer Emergency Response Teams, Security Focus,) and **maintain** currency of knowledge on the relevant legislation, regulations, methods, techniques etc.
Monitor, **analyze** and **evaluate** cyber threat actors targeting the organisation
Monitor, **analyze** and **evaluate** intrusion artifacts and **design** and **implement** mitigation actions (of potential cyber defense incidents) within the enterprise.
Monitor, analyze and **evaluate** network alerts from various sources within the enterprise.
Monitor, **analyze** and **report** on cyber defense trends.
Monitor, analyze, assess and evaluate the current cybersecurity status of the organization.
Monitor, analyze, assess and evaluate the cybersecurity compliance of the organization.
Monitor, **assess**, **evaluate** and **assure** the performance of the implemented cybersecurity controls.
Monitor, **evaluate, document** and **communicate** (as needed) training effectiveness and individual trainee's performance.
Monitor, **measure** and **evaluate** the effectiveness of implemented cybersecurity controls and risk levels.
Organise, **design** and **deliver** cybersecurity and data protection awareness-raising activities, seminars, courses and practical training to meet needs.
Organise, **design** and **deliver** cybersecurity and data protection awareness-raising activities, seminars, courses and practical training to meet needs.
Participate in mentoring, supervision and sharing activities as needed.
Organise, **design** and **deliver** cybersecurity simulations, virtual labs or cyber range environments.
Oversee, monitor and **safeguard** the quality of related assessments.
Perform (Implement) and m**onitor** audits against cybersecurity-related applicable laws, regulations and standards, **collect** needed evidence and **document** audit information and results, in alignment to the relevant audit plan(s).
Perform (Implement) audits against cybersecurity-related applicable laws, regulations and standards, **collect** needed evidence and **document** audit information and results, in alignment to the relevant audit plan(s).
Perform (Implement) tests against cybersecurity-related applicable laws, regulations and standards, **collect** needed evidence and **document** test information and results, in alignment to the relevant test plan(s).
Perform training needs analyses.
Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).
Preserve and **protect** digital evidence and make it available to authorized stakeholders.
Promote continuous enhancement of cybersecurity capacities and capabilities building.
Secure and **manage** the budget for cybersecurity.
Securely **configure** systems, services and products.
Set up (establish) and **manage** a suitable environment for the secure development of systems, services and products components, throughout the entire lifecycle.
Support the development and coordination of partnerships with external stakeholders and organisations.
Support users and other related parties as needed on cybersecurity-related issues.
Translate business requirements into Intelligence requirements.
Update cybersecurity audit plan(s) including their needed components (frameworks, standards, methodologies, procedures, tests, objectives, etc.) based on context changes (technological landscape, regulations and the organisation's IT assets and technologies).

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

2.2. SKILLS

2.2.1. Action verbs on skills

Advise: to give someone useful information, or to tell them what you think they should do[li]
Adapt: to change, or to change something, to suit different conditions or uses[lii]
Align: to change something so that it has a correct relationship to something else[liii]
Analyze: to study or examine something in detail in order to discover or understand more about it[liv]
Anticipate: to take action in preparation for something that you think will happen[lv]
Apply: to make use of something or use it for a practical purpose[lvi]
Automate: to make something operate automatically by using machines or computers[lvii]
Author: to write a book, article, etc[lviii]
Assess: to judge or decide the amount, value, quality, or importance of something[lix]
Assist: to take action to help someone or support something[lx]
Audit: systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled[lxi]
Build: the process of creating a version of a piece of software, etc.[lxii]
Capture: to represent or describe something very accurately using words or images[lxiii]
Categorise: categorize sth into sth[lxiv]
Communicate: to share information with others by speaking, writing, or using other signals[lxv]
Configure: to arrange something or put its parts together in a particular form or arrangement[lxvi]
Conduct: to organize and perform a particular activity[lxvii]
Convey: to express a thought, feeling, or idea so that it is understood by other people[lxviii]
Contribute: to add new plans or ideas, or help make improvements to something so that it becomes more valuable or successful[lxix]
Coordinate: to make many different things work effectively as a whole[lxx]
Cooperate: to act or work together for a particular purpose, or to be helpful by doing what someone asks you to do[lxxi]
Correlate: relate (sth) with sth[lxxii]
Define: to explain and describe the meaning and exact limits of something[lxxiii]
Deliver: to give or produce a speech or result[lxxiv]
Design: to decide how something will look, work, etc., by drawing plans, making computer models, etc.[lxxv]
Determine: to find out or make certain facts or information[lxxvi]
Develop: to (cause something to) grow or change into a more advanced, larger, or stronger form[lxxvii]
Direct: to control or be in charge of an activity, organization, etc.[lxxviii]
Disseminate: to spread or give out something, especially news, information, ideas, etc., to a lot of people[lxxix]
Document: to record the details of an event, a process, etc.[lxxx]
Enable: to make someone able to do something, or to make something possible[lxxxi]

Enhance: to improve the quality, amount, or strength of something[lxxxii]
Ensure: to make something certain to happen[lxxxiii]
Establish: to discover or get proof of something[lxxxiv]
Evaluate: to judge or calculate the quality, importance, amount, or value of something[lxxxv]
Explain: to make something clear or easy to understand by describing or giving information about it[lxxxvi]
Follow: to obey someone, or to act according to something[lxxxvii]
Gauge: to make a judgment about something[lxxxviii]
Guide: to show someone how to do something difficult[lxxxix]
Identify: to recognize a problem, need, fact, etc. and to show that it exists[xc]
Implement: to put a plan/policy/measure into action[xci]
Improve: to (cause something to) get better[xcii]
Incentivize: to make someone want to do something[xciii]
Influence: to affect or change how someone or something develops, behaves, or thinks[xciv]
Integrate: to combine two or more things in order to become more effective[xcv]
Interpret: to decide what the intended meaning of something is[xcvi]
Lead: to control a group of people, a country, or a situation[xcvii]
Manage: coordinated activities to direct and control an organization[3xcviii]
Maintain: to keep something in good condition[xcix]
Monitor: determining the status of a system, a process, a product, a service, or an activity
Operate: to (cause to) work, be in action or have an effect[c]
Organize: to make arrangements for something to happen[ci]
Perform: to do an action or piece of work[cii]
Plan: a set of decisions about how to do something in the future[ciii]
Practice: to do something regularly[civ]
Prepare: to make or get something or someone ready for something that will happen in the future[cv]
Preserve: to keep something as it is, especially in order to prevent it from decaying or being damaged or destroyed[cvi]
Promote: to encourage or support something, or to help something become successful[cvii]
Propose: to offer or suggest a possible plan or action for other people to consider[cviii]
Protect: to keep someone or something safe from injury, damage, or loss[cix]
Provide: to give someone something that they need[cx]
Predict: to say that an event or action will happen in the future, especially as a result of knowledge or experience[cxi]
Present: to give, provide, or make something known[cxii]
Recognise: to know someone or something because you have seen or experienced that person or thing before[cxiii]
Research: to study a subject in detail, especially in order to discover new information or reach a new understanding[cxiv]
Report: to give a description of something or information about it to someone[cxv]
Review: to think or talk about something again, in order to make changes to it or to make a decision about it[cxvi]
Secure: to make certain something is protected from danger or risk[cxvii]

[3] Management can include establishing policies and objectives, and processes to achieve these objectives

Select: to choose a small number of things, or to choose by making careful decisions[cxviii]
Solve: to find an answer to a problem[cxix]
Test: determination according to requirements for a specific intended use or application. Note 1 to entry: If the result of a test shows conformity, it can be used for purposes of validation[cxx].
Use: to put something into your service for a purpose[cxxi]
Verify: to prove that something exists or is true, or to make certain that something is correct[cxxii]
Work: to perform as intended or desired, or to cause something to do what it was intended to do[cxxiii]

2.2.2. List of skills

Once the gaps were identified, to ensure the use of the same language for the same skills, all profiles were deconstructed, and one list of skills (see the table below) was established. It was revised linguistically and content-wise to ensure that the same language was used in all the role profiles.

Table 3: List of skills

Skills description
Adapt and customise penetration testing tools and techniques.
Analyse and consolidate organisation's quality and risk management practices.
Analyse and **solve** complex problems and security challenges.
Analyse business processes, **assess** and **review** software or hardware security, as well as technical and organisational controls.
Analyse feasibility in terms of costs and benefits.
Analyse future developments in business process and technology application.
Analyse the company critical assets and identify weaknesses and vulnerability to intrusion or attack.
Anticipate future cybersecurity threats, trends, needs and challenges in the organization .
Anticipate required changes to the organisation's information security strategy and formulate new plans.
Apply auditing tools and techniques.
Apply critical reading/thinking skills and evaluate information for reliability, validity and relevance.
Apply ethical cybersecurity organisation requirements.
Apply network protection components and security controls .
Apply relevant standards, best practices and legal requirements for information security.
Apply security design principles, e.g. least privilege.
Apply social engineering techniques.
Assess and **enhance** an organisation's cybersecurity posture, propose effective contingency measures, perform security audits.
Assess existing quality standards and align processes and activities with IT product and service quality expectations.
Assess the extent to which emerging information technologies fit within a given architecture.
Assess the security and performance of solutions (perform and evaluate test results against product specifications, **verify** that integrated systems capabilities and efficiency match specifications).

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Skills description
Assist in communication of the enterprise architecture and standards, principles and objectives to the application teams.
Audit with integrity, being impartial and independent.
Automate threat intelligence management procedures.
Build a cybersecurity risk-aware environment.
Build resilience against paints of failure across the architecture .
Predict the probability of an outcome based on calculations or experience.
Carry out risk management processes and perform risk analysis to identify required preventive actions and apply mitigation techniques .
Carry out working-life practices of the data protection and privacy, as well as cybersecurity issues involved in the implementation of the organisational processes, finance and business strategy.
Collect information while preserving its integrity.
Collect, **analyse** and **correlate** cyber threat information originating from multiple sources.
Collect, **evaluate**, **maintain** and **protect** auditing information.
Communicate and **disseminate** the scientific outcomes.
Communicate and **promote** the organisation's risk analysis outcomes and risk management processes .
Communicate effectively to ensure appropriate resources are deployed internally or externally to minimise outages.
Communicate in a collaborative environment through different tools .
Communicate or **author** publications, reports and training material with the appropriate technical level of documentation.
Communicate, **coordinate** and **cooperate** with internal and external stakeholders.
Communicate, **explain** and **adapt** legal and regulatory requirements and business needs.
Communicate, **present** and **report**.
Conduct audits, **analyse** results and **implement** changes to adress identified gaps.
Conduct ethical hacking.
Conduct performance and resilience testing.
Conduct risk management audits and **act** to minimise exposures.
Conduct technical analysis and reporting.
Conduct user and business requirements analysis.
Conduct, **monitor** and **review** privacy and cybersecurity impact assessments using standards, frameworks, acknowledged methodologies and tools.
Configure solutions according to the organisation’s security policy (configure components at any level to guarantee correct performance, interoperability and security, organise secure solutions, security controls and configurations, apply security design principles, e.g. least privilege, build resilience against points of failure across the architecture, apply appropriate software and/or hardware and/or network architectures, design and develop network and hardware architecture, user interfaces, business software components and embedded software components, apply principals of security by design and defense in depth, add, remove, or update user account information, resetting passwords, etc., configure, add and delete file systems).
Continuously **monitor** new advancements and cybersecurity innovations .
Contribute to the development of ICT strategy and policy, including ICT security and quality.
Contribute to the identification of risks that arise from potential technical solution architectures. Suggests alternate solutions or countermeasures to mitigate risks. Defines secure systems configurations in compliance with intended architectures.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Skills description
Convey complex information, concepts, or ideas effectively through verbal, written, and/or visual means and to different levels of audience .
Coordinate the integration of security solutions.
Decompose, **analyse** systems, spot weaknesses, **develop** security and privacy requirements and **identify** effective or ineffective related solutions.
Define and **apply** maturity models for cybersecurity management, **apply** benchmarking and improvement/maturity models for security management.
Define, present and **promote** an information security policy for approval by the senior management of the organisation.
Deliver cybersecurity education and training.
Deliver training utilising various training resources.
Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles.
Design, **apply**, **monitor** and **review** Information Security Management System (ISMS) either directly or by leading its outsourcing.
Design, **develop** and **deliver** cybersecurity curricula and programmes to meet the organisation and individuals' needs.
Determine appropriate targeting options and identify critical target elements.
Determine requirements for processes related to ICT services.
Develop advanced cybersecurity exercises and scenarios for simulations, virtual or cyber range environments.
Develop and follow leads to assess evidence creatively.
Develop and **implement** solutions to practical, operational or conceptual problems which arise in the execution of work, in a wide range of contexts.
Develop and **implement** standard operating procedures based on IT policies and practices, ensuring compliance with standards and regulations.
Develop and **test** organisational resilience, including techniques for simulations and exercises.
Develop and **test** secure code and scripts (**conduct** performance and resilience testing, report and document tests and results, design tests of ICT systems, prepare and conduct tests of ICT systems including automation support, automate routine system administration tasks to specifications using standard tools and basic scripting).
Develop codes, scripts and programmes.
Develop detailed and reasoned investigation reports.
Develop evaluation programs for the awareness, training and education activities.
Develop, **apply** and **evaluate** algorithms, predictive data modelling and data visualisation to identify underlying trends and patterns in data.
Develop, champion and **lead** the execution of a cybersecurity strategy.
Draw architectural and functional specifications .
Enable business assets owners, executives and other stakeholders to make risk informed decisions to manage and mitigate risks.
Enable employees to understand, embrace and follow the controls.
Ensure best architecture solutions are implemented.
Establish a cybersecurity plan.
Establish the recovery plan.

Skills description
Explain and **communicate** data protection, privacy and cybersecurity compliance topics to stakeholders and users.
Explain and **present** digital evidence in a simple, straightforward and easy to understand way.
Follow and **practice** auditing frameworks, standards and methodologies.
Gauge learner understanding and knowledge level and, **provide** effective feedback to students for improving learning.
Generate new ideas and transfer theory into practice .
Guide and **communicate** with implementers and IT/OT personnel.
Identify and **exploit** vulnerabilities.
Identify and model treats, actors, TTPs and campaigns.
Identify and **select** appropriate pedagogical approaches for the intended audience.
Identify needs in cybersecurity awareness, training and education.
Identify non-cyber events with implications on cyber-related activities.
Identify systems weaknesses and security risks.
Identify underlying trends and patterns in business data using statistical and computational techniques and tools.
Identify, **analyse** and **correlate** events.
Identify, **troubleshoot** and **respond** to cybersecurity-related issues (provide expertise to help solve complex technical problems and ensure best architecture solutions are implemented, analyse symptoms to identify broad area of user error or technical failure, deploy support tools to systematically trace source of error or technical failure, analyse system logs and identifying potential hardware- or security issues with computer systems).
Identify, **capture**, **contain**, and **report** malware.
Implement cybersecurity risk management frameworks, methodologies and guidelines and **ensure** compliance with regulations and standards.
Implement the recovery plan in case of incident.
Influence an organisation's cybersecurity culture.
Integrate cybersecurity solutions to the organisation's infrastructure (use knowledge in various technology areas to build and deliver the enterprise architecture, secure/ back-up data to ensure integrity during system integration).
Interpret mathematical information.
Align publications to the solution during the entire lifecycle.
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.
Maintain a risk inventory' or register, prevent, monitor and recover from incidents.
Maintain psychological well-being.
Manage and **analyze** log files.
Manage cybersecurity resources and related budget.
Manage financial and material resources, undertake effective financial planning, using credit, savings, investments and pensions to achieve short and long term goals, using financial advices and guidance services with a critical mindset, comparing deals and offers when acquiring products or services and actively selecting appropriate insurance products.
Manage the threat intelligence ecosystem (from the procedures to the sharing of actionable information).

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Skills description
Monitor and **assess** the potential impact of emerging technologies on laws, regulations, and/or policies.
Monitor evolving security and privacy infrastructures, technologies and methods.
Monitor progress of issues throughout lifecycle and communicate effectively.
Motivate and **incentivise** learners.
Operate, **maintain**, **monitor**, **document** and **ensure** the performance of the implemented cybersecurity controls (measure system performance before, during and after system integration, document and record activities, problems and related repair activities, monitor progress of issues throughout lifecycle and communicate effectively).
Organise and **work** in a systematic and deterministic way based on evidence.
Organise, **lead** and **manage** cybersecurity related teams within organization.
Organize and **manage** intelligence development process in accordance to relevant requirements.
Perform damage and risk assessments (for the specific incidents and the related scenarios).
Perform basic risk assessments for small information systems.
Plan and **conduct** interviews in a systematic and deterministic manner.
Plan and **organize**. **Direct** activities and tasks, **establish** schedules and **coordinate** the activities of groups and individuals to complete objectives on time and within budget.
Practice all technical, functional and operational aspects of cybersecurity incident handling and response.
Prepare and **conduct** tests of ICT systems including automation support.
Prepare the data / relevant information for sharing in accordance to relevant policies.
Preserve evidence integrity according to standard operating procedures or national standards.
Process information, ideas and concepts, evaluate, input, record, transcribe and update data using electronic or manual information systems.
Propose and **manage** risk-sharing options.
Propose cybersecurity architectures based on stakeholder's needs and budget.
Protect a network against malware (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
Prove the soundness of the research results.
Provide expertise to help solve complex technical problems and ensure best architecture solutions are implemented.
Provide practical solutions to cybersecurity issues.
Provide technological design leadership.
Recognize and **categorize** types of vulnerabilities and associated attacks.
Report and **document** tests and results.
Report, **communicate** and **present** to stakeholders.
Research, understand, act up on, **resolve** security vulnerabilities (analyse the company critical assets and identify weaknesses and vulnerability to intrusion or attack, Implement change management procedures, report and document tests and results).
Review and **enhance** security documents, reports, SLAs and ensure the security objectives.
Review current practices of performing IT-related activities, and **propose** revisions to service standads and protocols.
Secure network communications.
Select appropriate specifications, procedures and controls.
Self-management skills and competences.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Skills description
Solve and **troubleshoot** problems.
Strictly and systematically **follow** the prescribed procedures.
Think creatively and innovatively.
Understand, **analyse** and **implement** cybersecurity risk management, design and document the precesses for risk analysis and management.
Understand, **analyse** and **implement** cybersecurity standards, frameworks, policies, regulations, legislations, certifications and best practices.
Understand, practice and **follow** to ethical requirements and standards.
Use security event correlation tools.
Use cybersecurity techniques, methods and tools for auditing systems and, **perform** reverse-engineering and forensic analysis.
Use penetration testing tools effectively.
Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc).
Use, **assess** and **apply** relevant CTI platforms, databases and tools.
Work across departments and business units to implement organization's privacy principles and programs and align privacy objectives with security objectives.
Work ethically, following codes of professional ethics or other equivalent.
Work in a team and cooperate with colleagues and different external partners.
Work independently, not influenced and biased by internal or external actors.
Work efficiently.
Work with digital devices and applications.
Develop and **communicate** intelligence reports to stakeholders.

2.3. KNOWLEDGE

Once the gaps were identified, to ensure the use of the same language for the same kowledge, all profiles were deconstructed, and one list of knowledge (see the table below) was established. It was revised linguistically and content-wise to ensure that the same language was used in all the role profiles.

Table 4: List of knowledge descriptors

Knowledge description
Knowledge of application protocols and services.
Knowledge of architectural design principles (e.g. operating models].
Knowledge of architecture frameworks, methodologies and systems design tools.
Knowledge of assembly and low-level programming interfaces.
Knowledge of asset management (hardware components, tools and architectures, physical devices like sensors, actors, the organisation's overall ICT /OT infrastructure and key components, key concepts and best practice in asset security).

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Knowledge description
Knowledge of auditing frameworks, standards, methodologies and certifications.
Knowledge of best practices on cybersecurity.
Knowledge of BYOD, security issues, common technical and user issues.
Knowledge of business continuity and disaster recovery continuity of operations plans.
Knowledge of business continuity and disaster recovery management processes, frameworks, standards, best practices and terminology.
Knowledge of business risk management.
Knowledge of capacity management and load balancing.
Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
Knowledge of cyber defense and information security policies, procedures, standards and regulations.
Knowledge of cybersecurity attack vectors.
Knowledge of cybersecurity awareness, education and training programme development.
Knowledge of cybersecurity frameworks, methodologies, controls and best practices.
Knowledge of cybersecurity maturity models.
Knowledge of cybersecurity methods, methodologies, tools and techniques.
Knowledge of cybersecurity solutions, outputs and integrity to comprehensive cybersecurity concept.
Knowledge of cybersecurity solutions, technical and organisational controls.
Knowledge of cybersecurity tactics, techniques and procedures.
Knowledge of cybersecurity threats, vulnerabilities and risks (including threats taxonomies and vulnerabilities repositories).
Knowledge of cybersecurity-related legislation, policies, regulations or governance specific for critical infrastructures.
Knowledge of cybersecurity-related professional certification schemes and certificates.
Knowledge of cybersecurity-related standards and compliance requirements.
Knowledge of cybersecurity-related technologies and controls.
Knowledge of cloud service models and how those models can limit incident response.
Knowledge of cloud, serverless, virtual private networks and on premise technologies.
Knowledge of company's enterprise architecture and its interconnection to networks.
Knowledge of compliance (legal) requirements and practices.
Knowledge of compliance assessment methodologies.
Knowledge of computer networks security (including. IoT. LAN. WLAN, mobile. Bluetooth, components, topologies, protocols, interconnections, B6K6 cloud and platform business models like SaaS. PaaS. IaaS).
Knowledge of copyright and intellectual property rights issues, standards and patent filing.
Knowledge of costs, benefits and risks of a system architecture.
Knowledge of criminal investigation methodologies and procedures.
Knowledge of critical threats, vulnerabilities and controls for the organisation's information provision.
Knowledge of CTI sharing standards.
Knowledge of cutting-edge methods, tools and techniques on hands-on cybersecurity education and training.
Knowledge of data (including big data) handling and analytics methods.
Knowledge of data protection and data privacy legislation, policies and regulations.
Knowledge of cyber security-related legislation, policies and regulations.
Knowledge of data storage, processing and protections within systems, services and infrastructures.

Knowledge description
Knowledge of DBMS, Data Warehouse, DSS.
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
Knowledge of different service models (SaaS, PaaS, laaS) and operational translations (i.e. Cloud Computing].
Knowledge of different sorts of tests (functional, integration, performance, usability, accessibility, security, stress etc.), national and international standards defining quality criteria for testing, testing methods, tools and automation including agile approaches, vulnerability and misuse testing.
Knowledge of digital forensics analysis and testing techniques, best practices and tools (extracting, reversing and understanding code and traces, logs).
Knowledge of elements forming the metrics of service level agreements.
Knowledge of enterprise architecture.
Knowledge of espionage and coercion threats and risks.
Knowledge of ethical cybersecurity organisation requirements.
Knowledge of ethical issues, rules and constraints.
Knowledge of ethical issues, rules and constraints regarding forensics investigation.
Knowledge of existing and emerging technologies (e.g. cloud, distributed ledger technologies. loT, AI, open data) and their security characteristics.
Knowledge of existing applications and related architecture.
Knowledge of functional & technical designing.
Knowledge of funding programs and grants.
Knowledge of ICT internal audit approach.
Knowledge of identified vulnerabilities and common methods of attack.
Knowledge of identity management, systems configuration, virtualization, networking management.
Knowledge of incident management processes, handling methodologies, best practices and terminology.
Knowledge of information and IT security strategy of the company.
Knowledge of information security.
Knowledge of intelligence disciplines, eco-system and methodologies.
Knowledge of interviewing techniques.
Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
Knowledge of IT technologies and network security methodologies.
Knowledge of IT/OT appliances, operating systems and computer networks.
Knowledge of key concepts and best practice in asset security.
Knowledge of key processes methods and principles to audit and security assessment.
Knowledge of latest cybersecurity trends (new and emerging information technology (IT) and cybersecurity technologies, emerging security issues, threats, vulnerabilities and risks).
Knowledge of legacy security techniques.
Knowledge of legal framework for digital evidence creation and conservation.
Knowledge of malware analysis concepts and methodologies.
Knowledge of malware analysis tools.
Knowledge of management practices.
Knowledge of mobile technologies.
Knowledge of mobility strategy.
Knowledge of monitoring, implementing, testing and evaluating the effectiveness of the controls.

Knowledge description
Knowledge of multidiscipline aspect of cybersecurity.
Knowledge of network environments, including field buses.
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
Knowledge of network services and protocols interactions that provide network communications.
Knowledge of network's attack techniques and a network attack's relationship to threats and vulnerabilities.
Knowledge of offensive and defensive security practices.
Knowledge of operating systems security (database management systems, Operating Systems and software platforms (including managed services and APIs).
Knowledge of operating systems, networking protocols and services.
Knowledge of organisation processes including, decision making, budgets and management structure.
Knowledge of organisation's architecture/infastructure.
Knowledge of organisation's mission and business objectives and risks.
Knowledge of organisation's overall ICT infrastructure and key components.
Knowledge of organisation's security incident management and recovery.
Knowledge of organisation's security' management policy and its implications for business processes and engagement with customers, suppliers and subcontractors.
Knowledge of OSI model, underlying network protocols (e.g., TCP/IP), Dynamic Host Configuration, Domain Name System (DNS), and directory services.
Knowledge of pedagogical methods, learning styles and modes of learning.
Knowledge of penetration testing tools, techniques and methodologies.
Knowledge of potential and opportunities of relevant standards and best practices.
Knowledge of principles, models, methods and techniques of risk management and risk analysis.
Knowledge of principles, standards and techniques for SIEM.
Knowledge of privacy impact assessment methodologies.
Knowledge of privacy-by-design methodologies.
Knowledge of privacy-enhancing technologies (PET).
Knowledge of programming languages.
Knowledge of project management and budgeting, risk management.
Knowledge of recent vulnerability disclosures, data breach incidents and geopolitical events impacting cyber risks.
Knowledge of relevant laws, regulations and industry standards.
Knowledge of research, development and innovation (RDI) relevant to cybersecurity subject matters.
Knowledge of resource management.
Knowledge of responsible disclosure of cybersecurity-related information.
knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices.
Knowledge of risk management terms (principles, models, methods, tools and techniques of risk management and risk analysis, economics of security & risk management).
Knowledge of risk sharing options and best practices.
Knowledge of scripting and programming languages.
Knowledge of scripting languages.

Knowledge description
Knowledge of secure coding practices (development tools (e.g. development environment, management, source code access/revision control), known vulnerabilities and secure code/component libraries.
Knowledge of secure software development lifecycle.
Knowledge of security approach in information strategy of the organisation.
Knowledge of security architecture reference models and security solutions.
Knowledge of security controls (principles and techniques for access management, principles of systems and data security, web, cloud and mobile technologies and conditions for effective and secure implementation).
Knowledge of security controls frameworks and standards.
Knowledge of security technologies and solutions.
Knowledge of security-related standards and requirements.
Knowledge of system administration, network, and operating system hardening techniques.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
Knowledge of systems and services provisioning, monitoring, scripting and logging.
Knowledge of systems development life cycle (best practice design techniques, requirement engineering, technical designing).
Knowledge of SLA documentation.
Knowledge of standards for documentation, information and content management, documentation reviews and tests.
Knowledge of statistics and forecasting methodologies.
Knowledge of storage management and database administration.
Knowledge of target methods and procedures.
Knowledge of TCP/IP networking.
Knowledge of technical and organisational controls that appropriately mitigate cybersecurity risks.
Knowledge of test methodologies and practices (integration testing techniques, techniques, infrastructure and tools to be used in the testing process, the lifecycle of a testing process).
Knowledge of threats modelling techniques.
Knowledge of tools, techniques and methods for learning assessment and evaluation.
Knowledge of troubleshooting processes and procedures.
Knowledge of TTP frameworks.
Knowledge of vulnerability and misuse testing.

3. REWIRE PROFILES

As described above, ensure the use of the same language for the same knowledge, all profiles were deconstructed, and one list of tasks, skills and knowledge was established. It was revised linguistically and content-wise to ensure that the same language was used in all the role profiles. Competences, skills, and knowledge were combined with the tasks attached to a particular role profile (see part 3). Then the final set of competences, skills, and knowledge were compared against the skills, knowledge and competences identified in the v0.5 of the ECSF.

The following tables contains the information of the Role profiles. In the column REWIRE the information that was produced by the activities of the working groups on the Cybersecurity Skills Framework are contained. To facilitate easier understanding on the proposals of the REWIRE project, the following symbols are used:

?	When information is added to that already displayed (existing) in the ENISA, ECSF, v0.5. in the same section, the symbol ? precedes the relevant information in the respective REWIRE column.
?	If the REWIRE proposes an adaptation or some changes to that already displayed (existing) in the ENISA, ECSF, v0.5. in the same section, the symbol ? precedes the relevant information in the respective REWIRE column.
–	If the REWIRE proposes the removal of some of the already displayed (existing) in the ENISA, ECSF, v0.5., then the – precedes the relevant information in the respective ENISA, ECSF, v0.5. respective column. The information contained in the REWIRE column does not follow a specific sequence.
EMPTY	If no additional information is proposed, the respective space in the REWIRE column is left empty. In the case where some of the tasks, skills, knowledge or e-competences are proposed by the REWIRE project to be retained, then no bullet or other symbol is displayed preceding them in the REWIRE column. This was done in the hope that it will be easier to read and comprehend.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.1. CHIEF INFORMATION SECURITY OFFICER (CISO)

Table 5: Comparison of ECSF (v.0.5) and REWIRE Chief information security officer profile

Source	**ENISA, ECSF, v0.5.**	**REWIRE**
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Programme Director Information Security Officer (ISO) Head of Information Security IT Security Officer	✚ Information Security Manager ✚ Chief ICT Security Officer ✚ ICT security manager ✚ Information systems security manager
Summary statement *Indicates the main purpose of the profile.*	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.	
Mission *Describes the rationale of the profile.*	Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	Cybersecurity Strategy Cybersecurity Policy	✚ Cybersecurity Policies, Procedures, Plans, Standards and Guidelines
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organizational objectives. Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution. Supervise the application and improvement of the Information Security Management System (ISMS). Educate senior management about cybersecurity risks, threats and their impact to the organization. Ensure the senior management approves the cybersecurity risks of the organization. Develop cybersecurity plans. Develop relationships with cybersecurity-related authorities and communities. Report cybersecurity incidents, risks, findings to the senior management. Monitor advancement in cybersecurity. Secure resources to implement the cybersecurity strategy. Negotiate the cybersecurity budget with the senior management. Ensure the organisation's resiliency to cyber incidents. Manage continuous capacity building within the organization. Review, plan and allocate appropriate cybersecurity resources.	? Design, develop, implement and manage cybersecurity policies, processes, procedures, standards, plans, guidelines and frameworks (including roles and responsibilities) in alignment with the business strategy to support the organizational objectives. ? Educate, monitor and assess the awareness of organization members as needed. ? Document, report and communicate (for information and approval where needed) the cybersecurity vision, strategy and risks (risk appetite, residual risk etc) to top management. ? Document and communicate effectively to Top Management as needed on cybersecurity incidents, risks, findings. ? Advise the top Management on the economics of cybersecurity. ? Design, develop, implement, manage and continually improve the information security management system. ? Monitor advancement in cybersecurity and the internal and external context. ? Monitor, analyze, assess and evaluate the cybersecurity compliance of the organization. ? Document and communicate to Top Management as needed on cybersecurity incidents, risks, findings. ✚ Monitor, analyze, assess and evaluate the current cybersecurity status of the organization

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.	REWIRE
		✚ Oversee, monitor and safeguard the quality of related assessments. ✚ Advise, support and coordinate with internal stakeholders on subjects related to cybersecurity and privacy compliance requirements. ✚ Design, document and implement cyber incident management policies, procedures and plans. ✚ Establish relationships, collaborate and communicate with stakeholders as needed (including cybersecurity-related authorities and communities). ✚ Secure and manage the budget for cybersecurity. ✚ Assist in the design, development, implementation and management of disaster recovery, business continuity and incident response policies, procedures, plans, standards and guidelines. ✚ Assist in the design, development, implementation and management of Risk Management within the organization. Have ownership and overview of the Risk Management process.
Key skill(s) *A list of abilities to perform work functions and duties by the profile. Ability to:*	Understand core organisational business processes. Assess and enhance an organisation's cybersecurity posture. Analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications and best practices. Manage cybersecurity resources. Develop, champion and lead the execution of a cybersecurity strategy Influence an organisation's cybersecurity culture 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 Practice ethical cybersecurity organisation requirements Provide practical solutions to cybersecurity issues Establish a cybersecurity plan Communicate, coordinate and cooperate with internal and external stakeholders Apply relevant standards, best practices and legal requirements for information security Anticipate required changes to the organisation's information security strategy and formulate new plans Define and apply maturity models for cybersecurity management. Anticipate future cybersecurity threats, trends, needs and challenges in the Organization. Ability to lead multidisciplinary cybersecurity teams.	Understand core organisational business processes. Review and enhance security documents, reports, SLAs and ensure the security objectives. Apply relevant standards, best practices and legal requirements for information security. Establish a cybersecurity plan. ? Understand the results of assessments and the possible impact of findings & interpret security analytics. ? Assess and enhance an organisation's cybersecurity posture, propose effective contingency measures, perform security audits. ? Understand, analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications and best practices. ? Analyse feasibility in terms of costs and benefits. ? Manage cybersecurity resources and related budget. ? Manage financial and material resources. Undertake effective financial planning, using credit, savings, investments and pensions to achieve short- and long-term goals, using financial advices and guidance services with a critical mindset, comparing deals and offers when acquiring products or services and actively selecting appropriate insurance products. ? Develop, champion and lead the execution of a cybersecurity strategy. ✚ Understand, analyse and implement management of cybersecurity related issues. Design and document processes for risk analysis and management. ✚ Maintain a risk inventory' or register, prevent, monitor and recover from incidents ✚ Communicate and promote the organisation's risk analysis outcomes and risk management processes

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.	REWIRE
		✚ Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing ✚ Communicate, coordinate and cooperate with internal and external stakeholders ✚ Assist in communication of the enterprise architecture and standards, principles and objectives to the application teams ✚ Analyse future developments in business process and technology application ✚ Anticipate future cybersecurity threats, trends, needs and challenges in the Organization ✚ Develop and test organisational resilience, including techniques for simulations and exercises. ✚ Influence an organisation's cybersecurity culture ✚ Perform security audits. ✚ Define and apply maturity models for cybersecurity management, apply benchmarking and improvement maturity models for security management. ✚ Provide expertise to help solve complex technical problems and ensure best architecture solutions are implemented. ✚ Apply security design principles, e.g. least privilege ✚ Build resilience against points of failure across the architecture. ✚ Anticipate required changes to the organisation's information security strategy and formulate new plans ✚ Establish the recovery plan ✚ Implement the recovery plan in case of incident ✚ Estimate the probability of an outcome based on calculations or experience. estimate the probability of an outcome or fact make estimations work with probabilities ✚ Practice ethical cybersecurity organisation requirements ✚ Preserve evidence integrity according to standard operating procedures or national standards. ✚ Process incident reports for prevention ✚ Fill in an incident report after a cybersecurity incident has happened at the company or facility based on industry best practices, legal and regulatory requirements and the organization's own policies and procedures. ✚ Monitor Assessment. Monitoring the assessment process related to quality and cybersecurity. ✚ Facilitate communication between organisations and interested third parties such as suppliers, distributors, shareholders and other stakeholders in order to inform them of the organisation and its objectives. ✚ Lead multidisciplinary cybersecurity teams, manage communication in a multi-disciplinary team ✚ Express and exchange information, ideas, concepts, thoughts, and feelings, and resolve disagreements in formal and informal contexts, through the use of shared systems of words, signs, and rules. ✚ Guide, direct and motivate others.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.	REWIRE
		✚ Process information, ideas and concepts. Evaluate, input, record, transcribe and update data using electronic or manual information systems. ✚ Direct activities and tasks, establish schedules and coordinate the activities of groups and individuals to complete objectives on time and within budget.
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	Knowledge of cybersecurity and privacy standards, frameworks, policies, regulations, legislations, certifications and best practices Understanding of ethical cybersecurity organisation requirements Knowledge of security controls Knowledge of cybersecurity maturity models Knowledge of cybersecurity tactics, techniques and procedures Knowledge of resource management Knowledge of management practices Knowledge of risk management frameworks	Knowledge of cybersecurity maturity models. Knowledge of cybersecurity tactics, techniques and procedures. ? Knowledge of security controls frameworks and standards. ? Understand core organisational business processes. ? Knowledge of compliance (legal) requirements and practices. ? Knowledge of identified vulnerabilities and common methods of attack. ? Knowledge of principles, models, methods and techniques of risk management and risk analysis. ? Knowledge of resource management ? Knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices. ? Knowledge of risk management terms (principles, models, methods, tools and techniques of risk management and risk analysis, economics of security & risk management). ? Knowledge of critical threats, vulnerabilities and controls for the organisation's information provision. ? Knowledge of security controls frameworks and standards ✚ Knowledge of data protection and data privacy legislation, policies and regulations ✚ Knowledge of ICT capacity planning strategies. The methods, techniques and ICT tools used for planning the maximum amount of work that an organisation is capable of completing in a given period, based on the number of machines, workers and shifts and taking into account constraints such as quality problems, delays and material handling. ✚ Knowledge of architectural design principles (e.g. operating models) ✚ Knowledge of enterprise architecture ✚ Knowledge of business continuity and disaster recovery plans, processes, frameworks, standards, best practices and terminology. ✚ Knowledge of cyber defense and information security policies, procedures, standards and regulations ✚ Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks) ✚ Knowledge of cybersecurity-related legislation, policies, regulations, standards, certifications and best practices ✚ Knowledge of DBMS, Data Warehouse, DSS ✚ Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks)

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.	REWIRE
		✚ Knowledge of different service models (SaaS, PaaS, IaaS) and operational translations (i.e. Cloud Computing] ✚ Knowledge of different sorts of tests (functional, integration, performance, usability, accessibility, security, stress etc.) ✚ Knowledge of elements forming the metrics of service level agreements ✚ Knowledge of enterprise architecture ✚ Knowledge of ethical cybersecurity organisation requirements. Knowledge of ethical issues, rules and constraints ✚ Knowledge of models and tools for cybersecurity planning and investment (e.g. Gordon-Loeb model, Return on security investment (ROSI) etc). ✚ Knowledge of offensive and defensive security practices ✚ Knowledge of organisation processes including, decision making, budgets and management structure ✚ Knowledge of organisation's overall ICT infrastructure and key components ✚ Knowledge of organisation's security incident management and recovery ✚ Knowledge of organisation's security' management policy and its implications for business processes and engagement with customers, suppliers, and subcontractors ✚ Knowledge of potential and opportunities of relevant standards and best practices ✚ Knowledge of secure software development lifecycle ✚ Knowledge of security approach in information strategy of the organisation ✚ Knowledge of SLA documentation ✚ Knowledge of storage management and database administration ✚ Knowledge of existing and emerging technologies (e.g. cloud, distributed ledger technologies. IoT, AI, open data) and their security characteristics ✚ Knowledge of existing applications and related architecture ✚ Knowledge of ICT internal audit approach ✚ Knowledge of identity management, systems configuration, virtualization, networking management ✚ Knowledge of incident management processes, handling methodologies, best practices and terminology ✚ Knowledge of key concepts and best practice in asset security ✚ Knowledge of BYOD, security issues, common technical and user issues ✚ Knowledge of capacity management and load balancing ✚ Knowledge of cloud, serverless, virtual private networks and on-premise technologies ✚ Knowledge of management practices ✚ Knowledge of mobile technologies and of mobility strategy ✚ Knowledge of systems and services provisioning, monitoring, scripting and logging ✚ Knowledge of the hierarchy of documentation (policies, procedures, standards, guidelines etc)

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.		REWIRE	
			✚ Knowledge of the organization, its processes regarding financial management, procurement, and HR processes. ✚ Knowledge of the process of planning, monitoring, and adjusting the expenses and revenues of a function / department / division in order to achieve cost efficiency and capability. ✚ Knowledge of the relevant cost estimation and effectiveness of cybersecuirty controls, mechanisms, and tools ✚ Knowledge of threats modelling techniques ✚ Knowledge of troubleshooting processes and procedures ✚ Knowledge of vulnerability and misuse testing ✚ Understand core organisational business processes.	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	D.1. Information Security Strategy Development E.3. Risk Management E.4. Relationship Management E.8. Information Security Management E.9. IS-Governance	Level 5 Level 4 Level 3 Level 4 Level 4	✚ A.1. Information Systems and Business Strategy Alignment ✚ A.2. Service Level Management ✚ A.5. Architecture Design ✚ B.5. Documentation Production ✚ C.4. Problem Management D.1. Information Security Strategy Development E.3. Risk Management E.4. Relationship Management ✚ E.7. Business Change Management E.8. Information Security Management E.9. IS-Governance ✚ A.6. Application Design (Optional) ✚ B.3. Testing (Optional) ✚ C.5. Systems Management (Optional)	Level 5 Level 4 Level 3 Level 3 Level 4 Level 5 Level 4 Level 3 Level 4 Level 4 Level 4 Level 1 Level 1 Level 1

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.2. CYBER INCIDENT RESPONDER

Table 6: Comparison of ECSF (v.0.5) and REWIRE Cyber incident responder profile

Source	ENISA, ECSF, v0.5.	REWIRE
Alternative Title(s) *Lists titles under the same profile*	Cyber Incident Handler – Security Operations Center (SOC) Analyst Cyber Fighter /Defender – Log Files Analyst – Security Operation Analyst (SOC Analyst) – Cybersecurity SIEM Manager	? Incident response engineer ? Cyber incident / crisis manager ? Blue team member ? Incident management team member (white) ? Member of the IRT
Summary statement *Indicates the main purpose of the profile.*	– Monitor the organisation's cybersecurity state, manage incidents during cyber-attacks and assure the continued operations of ICT systems.	✚ Investigates, analyzes, and responds to cyber incidents within the network environment.
Mission *Describes the rationale of the profile.*	– Analyses, evaluates and mitigates the impact of cybersecurity incidents. Monitors and assesses systems' cybersecurity state. According to the organisation's Incident Response Plan, restores systems' and processes' functionalities to an operational state.	✚ Monitors the system including the infrastructure and the services for anomalies, performs preventive actions to mitigate vulnerabilities and corrective actions so as to mitigate the impact of cyber incidents. Identifies threats and root causes of incidents. Collects evidence, documents the incidents and actions taken, and develops strategies for avoiding future incidents
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	– Cyber Incident Management • Incident Response Plan – Recovery Process – Cyber Incident Report – Vulnerability Management	? Cyber security incident response plan
Main task(s) *A list of typical tasks performed by the profile. is tasked to:*	• Contribute to the development, maintenance and assessment of the Incident Response Plan – Develop, implement and assess procedures related to incident handling • Identify, analyse, mitigate and communicate cybersecurity incidents – Assess and manage technical vulnerabilities • Measure cybersecurity incidents detection and response effectiveness • Evaluate the resilience of the cybersecurity controls and mitigation actions taken after a cybersecurity or data breach incident • Adopt and develop incident handling testing techniques • Establish procedures for incident results analysis and incident handling reporting • Document incident results analysis and incident handling actions – Cooperate with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) • Cooperate with key personnel for reporting of security incidents according to applicable legal framework	? Design, document and implement cyber incident management policies, procedures and plans ? Design, document and communicate cyber defense techniques, guidance, and reports on incident findings as needed. ✚ Analyze, collect and evaluate evidence of possible security events and incidents. ✚ Coordinate and advise enterprise-wide cyber defense technicians on resolution of cyber defense incidents ✚ Coordinate incident response activities ✚ Document and communicate as needed after action reviews, lead the lessons learned sessions etc ✚ Monitor, analyze and evaluate intrusion artifacts and design and implement mitigation actions (of potential cyber defense incidents) within the enterprise ✚ Monitor, analyze and evaluate network alerts from various sources within the enterprise. ✚ Monitor, analyze and report on cyber defense trends.
Key skill(s) *A list of abilities to perform work functions and duties*	• Practice all technical, functional and operational aspects of cybersecurity incident handling and response • Work on operating systems, servers, clouds and relevant infrastructures – Work under pressure	Practice all technical, functional and operational aspects of cybersecurity incident handling and response ? Collect, analyze, manage and evaluate log files

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.	REWIRE
by the profile. *Ability to:*	• Command, communicate and report • Manage and analyse log files.	✚ Use security event correlation tools ✚ Preserve evidence integrity according to standard operating procedures or national standards. ✚ Protect a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters) ✚ Recognize and categorize types of vulnerabilities and associated attacks ✚ Secure network communications ✚ Perform damage and risk assessments (for the specific incidents and the related scenarios) identifying, capturing, containing, and reporting malware ✚ Recognize and categorize types of vulnerabilities and associated attacks
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of cybersecurity incident handling methodologies • Knowledge of cybersecurity incident handling practices and tools • Knowledge of incident handling communication cycle • Knowledge of operating systems internals, networking protocols and services • Knowledge of cybersecurity attacks tactics and techniques • Knowledge of cyber threats and vulnerabilities • Knowledge of legal framework related to cybersecurity and data protection • Knowledge of the operation of Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs)	Knowledge of the operation of Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) Knowledge of incident handling communication cycle Knowledge of cybersecurity incident handling practices and tools ? Knowledge of incident management processes, handling methodologies, best practices and terminology ? Knowledge of cyber defense and information security policies, procedures, standards and regulations ? Knowledge of network's attack techniques and a network attack's relationship to threats and vulnerabilities ✚ Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks) ✚ Knowledge of malware analysis concepts and methodologies ✚ Knowledge of offensive and defensive security practices ✚ Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions ✚ Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code) ✚ Knowledge of system administration, network, and operating system hardening techniques ✚ Knowledge of OSI model, underlying network protocols (e.g., TCP/IP), Dynamic Host Configuration, Domain Name System (DNS), and directory services ✚ Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth) ✚ Knowledge of network services and protocols interactions that provide network communications

Source	ENISA, ECSF, v0.5.		REWIRE	
			✚ Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks) ✚ Knowledge of cloud service models and how those models can limit incident response ✚ Knowledge of business continuity and disaster recovery continuity of operations plans	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.7. Technology Trend Monitoring B.2. Component Integration B.3. Testing B.5. Documentation Production C.4. Problem Management	Level 3 Level 2 Level 3 Level 3 Level 4	✚ D.1. Information Security Strategy Development ✚ D.10. Information and Knowledge Management ✚ A.9 Innovating ✚ E.8. Information Security Management A.7 Technology Trend Monitoring	Level 4 Level 4 Level 4 Level 4 Level 4

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.3. CYBER LEGAL, POLICY & COMPLIANCE OFFICER

Table 7: Comparison of ECSF (v.0.5) and REWIRE Cyber legal, policy and compliance officer profile

Source	**ENISA, ECSF, v0.5.**	**REWIRE**
Alternative Title(s) *Lists titles under the same profile*	Data Protection Officer (DPO) Privacy Protection Officer Cyber Law Consultant Information Governance Officer Data Compliance Officer Cybersecurity Lawyer IT Compliance Manager	Privacy Compliance Manager Cyber Legal Advisor Cyber Security Advice and Assessment
Summary statement *Indicates the main purpose of the profile.*	Manages compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organisation's strategy and legal requirements.	
Mission *Describes the rationale of the profile.*	Oversees and assures compliance with cybersecurity- and data-related legal, regulatory frameworks and policies in line with the organisation's strategy and legal requirements. Contributes to the organisation's data protection related actions. Provides legal advice in the development of the organisation's cybersecurity governance processes.	ensures their compliance with organisation's policies and procedures, prepares annual cybersecurity audit report for management (e.g. Chief Information Security Officer) identifying technical and procedural findings and providing recommended remediation strategies/solutions.
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Data Protection Policy	Cybersecurity Policy and Procedures Annual cybersecurity audit report
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations • Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures • Enforce and advocate organisation's data privacy and protection program • Ensure that data owners, holders, controllers, processors, subjects, internal or external partners and entities are informed about their data protection rights, obligations and responsibilities • Act as a key contact point to handle queries and complaints regarding data processing • Assist in designing, implementing, auditing and compliance testing activities in order to ensure cybersecurity and privacy compliance • Monitor audits and data protection related training activities • Cooperate and share information with authorities and professional groups • Contribute to the development of the organisation's cybersecurity strategy, policy and procedures	Enforce and advocate organisation's data privacy and protection program Act as a key contact point to handle queries and complaints regarding data processing Manage legal aspects of information security responsibilities and third-party relations. Conduct (wholly or partially) privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures. Cooperate and communicate with authorities and professional groups as needed. Design and Manage Cybersecurity Policies & Procedures in alignment with the business strategy to support the organizational objectives (Fully or partially). Educate, monitor and assess the awareness of organization members and external parties on cybersecurity and privacy issues as needed. Analyze, assess and evaluate the effectiveness of cybersecurity related policies, processes, procedures,

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	• Manage legal aspects of information security responsibilities and third-party relations	standards or practices in relation to relevant applicable laws and regulations. ? Perform (Implement) and Monitor audits against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document audit information and results, in alignment to the relevant audit plan(s). ? Advise, support and coordinate with internal stakeholders on subjects related to cybersecurity and privacy compliance requirements. ✚ Advise on, design, develop and update documents due to the introduction of existing, new or revised laws, regulations, executive orders, policies, standards, or procedures. ✚ Advise top management on risk levels and security posture. ✚ Advocate organization's official position in legal and legislative proceedings. ✚ Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance. ✚ Identify and interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program. ✚ Identify and resolve conflicts between relevant applicable laws and regulations and cybersecurity policies, processes, procedures, standards or practices. ✚ Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).
Key skill(s) *A list of abilities to perform work functions and duties by the profile. Ability to:*	– Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements – Abilities to carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy • 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 • Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools • Ability to explain and communicate data protection and privacy topics to stakeholders and users – Understand, practice and adhere to ethical requirements and standards – Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies – Work as part of a team and collaborate with colleagues	? Conduct (wholly or partially) privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures. ? Design and Manage Cybersecurity Policies & Procedures in alignment with the business strategy to support the organizational objectives (Fully or partially). ✚ Act as a key contact point to handle queries and complaints regarding data processing; ✚ Advise on, design, develop and update documents due to the introduction of existing, new or revised laws, regulations, executive orders, policies, standards, or procedures. ✚ Advise top management on risk levels and security posture. ✚ Advise, support and coordinate with internal stakeholders on subjects related to cybersecurity and privacy compliance requirements. ✚ Advocate organization's official position in legal and legislative proceedings. ✚ Analyze, assess and evaluate the effectiveness of cybersecurity related policies, processes, procedures, standards or practices in relation to relevant applicable laws and regulations.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

		✚ Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance. ✚ Cooperate and communicate with authorities and professional groups as needed. ✚ Educate, monitor and assess the awareness of organization members and external parties on cybersecurity and privacy issues as needed. ✚ Enforce and advocate organisation's data privacy and protection program ✚ Identify and interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program. ✚ Identify and resolve conflicts between relevant applicable laws and regulations and cybersecurity policies, processes, procedures, standards or practices. ✚ Manage legal aspects of information security responsibilities and third-party relations. ✚ Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery). ✚ Perform (Implement) and Monitor audits against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document audit information and results, in alignment to the relevant audit plan(s). ✚ Revise legal documents. Read and interpret legal documents and proofs about happenings in relation with the legal case. ✚ Compile legal documents. Compile and collect legal documents from a specific case in order to aid an investigation or for a court hearing, in a manner compliant with legal regulations and ensuring records are properly maintained. ✚ Meet deadlines for preparing legal cases. Plan and adjust timings in order to prepare legal documents, collect information and evidence, and contact clients and lawyers in order to prepare the case properly. ✚ Respect confidentiality obligations. Observe the necessary discretion and restraint when dealing with confidential, secret or unpleasant information.
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of information security • Advanced knowledge of data privacy and protection laws and regulations • Advanced knowledge of National, EU and international cybersecurity and related privacy standards, legislation, policies and regulations • Knowledge of legal compliance requirements and practices • Knowledge of privacy impact assessment methodologies • Basic understanding of data storage, processing and protections within systems, services and infrastructures	Knowledge of information security Knowledge of privacy impact assessment methodologies Knowledge of compliance (legal) requirements and practices Knowledge of data storage, processing and protections within systems, services and infrastructures ? Knowledge of privacy impact assessment methodologies knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices ✚ Knowledge of data protection and data privacy legislation, policies and regulations ✚ Knowledge of the organization's own data protection policies, procedures and practices

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			✚ Knowledge of the basic data protection principles and requirements. ✚ Knowledge of the data subjects' rights as described in relevant regulations and legislation. ✚ Knowledge of the policies of the organization in relation to data breach notification. ✚ Knowledge of critical threats, vulnerabilities and controls for the organisation's information provision ✚ Knowledge of potential and opportunities of relevant standards and best practices ✚ Knowledge of security controls frameworks and standards ✚ Knowledge of cybersecurity-related legislation, policies, regulations, standards, certifications and best practices ✚ Understand core organisational business processes ✚ Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies; ✚ Knowledge of security approach in information strategy of the organisation ✚ Knowledge of Legal and related matters as prescribed by the various national frameworks (in relation to the legal / attorney profession) ✚ Understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements; ✚ Knowledge of cybersecurity-related legislation, policies, regulations or governance specific for critical infrastructures ✚ Knowledge of cybersecurity maturity models ✚ Knowledge of ICT internal audit approach ✚ Knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices ✚ Knowledge of the hierarchy of documentation (policies, procedures, standards, guidelines etc) ✚ Knowledge on education and training ✚ Knowledge of the types of non-conformities and ways to correct them &The corrective actions process. ✚ Knowledge of the types of security related documents like reports, SLAs etc. ✚ Knowledge of legal case management. The procedures of a legal case from opening to closing, such as the documentation that needs to be prepared and handled, the people involved in different stages of the case, and the requirements that need to be met before the case can be closed. ✚ Knowledge of cybersecurity awareness, education and training programme development	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.1. Information Systems and Business Strategy Alignment D.1. Information Security Strategy Development E.8. Information Security Management E.9. IS-Governance	Level 4 Level 4 Level 3 Level 4	✚ Legal Government and Jurisprudence (NIST C30). A.1. Information Systems and Business Strategy Alignment ✚ C.4. Problem management D.1. Information Security Strategy Development ✚ D.3. Education and Training Provision	Level 4 Level 4 Level 2 Level 4 Level 2

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			✚ D.5. Documentation production ✚ D.10. Information and Knowledge Management ✚ E3. Risk management ✚ E.4. Relationship Management E.8. Information Security Management E.9. IS-Governance	Level 3 Level 4 Level 3 Level 3 Level 3 Level 4

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.4. CYBER THREAT INTELLIGENCE SPECIALIST

Table 8: Comparison of ECSF (v.0.5) and REWIRE Cyber threat intelligence specialist profile

Source	**ENISA, ECSF, v0.5.**	**REWIRE**
Alternative Title(s) *Lists titles under the same profile*	Cyber Intelligence Analyst Cyber Threat Modeller	
Summary statement *Indicates the main purpose of the profile.*	Collect, process, analyse data and information to produce actionable intelligence reports and disseminate them to target stakeholders.	
Mission *Describes the rationale of the profile.*	Manages 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. Identifies and monitors 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.	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cyber Intelligence Analysis • Cyber Threat Intelligence Management • Cyber Threat Report	
Main task(s) *A list of typical tasks performed by the profile. is tasked to:*	• Develop, implement and manage the organisation's cyber threat intelligence strategy • Develop plans and procedures to manage threat intelligence • Translate business requirements into Intelligence Requirements • Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders • Identify and assess cyber threat actors targeting the organisation • Identify, monitor and assess the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors by analysing open-source and proprietary data, information and intelligence • Produce actionable reports based on threat intelligence data • Elaborate and advise on mitigation plans at the tactical, operational and strategic level • Coordinate with stakeholders to share and consume intelligence on relevant cyber threats • Leverage intelligence data to support and assist with threat modelling, recommendations for Risk Mitigation and cyber threat hunting – Articulate and communicate intelligence openly and publicly	Translate business requirements into Intelligence requirements. Coordinate with stakeholders to share and consume intelligence on relevant cyber threats Design plans and procedures to manage threat intelligence ? Collect, analyze, produce and communicate actionable intelligence as needed. ? Identify, monitor and assess the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors, the model threats, actors and campaigns ? Monitor, analyze and evaluate cyber threat actors targeting the organization. ? Document and communicate as needed based on threat intelligence data ? Advise on mitigation plans at the tactical, operational and strategic level ? Advise on threat modelling, risk mitigation and cyber threat hunting based on intelligence data ? Design and manage the organisation's cyber threat intelligence strategy

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.	REWIRE
	at all levels – Convey the proper security severity by explaining the risk exposure and its consequences to non-technical stakeholders	✚ Design and Manage data management and sharing procedures and policies, taking into consideration relevant legal, regulatory, industry and company constraints ✚ Design and manage intelligence development process in accordance to relevant requirements ✚ Determine appropriate targeting options and identify critical target elements
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Work in a team and cooperate with different external Subject Matter Experts whenever needed • Collect, analyse and correlate cyber threat information originating from multiple sources • Identify threat actors TTPs and campaigns • Automate threat intelligence management procedures • Conduct technical analysis and reporting • Identify non-cyber events with implications on cyber-related activities • Model threats, actors and TTPs • Write and communicate intelligence reports to stakeholders • Use and apply CTI platforms and tools	Write and communicate intelligence reports to stakeholders Identify and model threats, actors, TTPs and campaigns Automate threat intelligence management procedures Conduct technical analysis and reporting Identify non-cyber events with implications on cyber-related activities Collect, analyse and correlate cyber threat information originating from multiple sources ? Use, assess and apply relevant CTI platforms, databases and tools. ? Work in a team and cooperate with different external partners setting intelligence process and operational environments. ✚ Determine appropriate targeting options and identify critical target elements ✚ Manage the threat intelligence ecosystem (from the procedures to the sharing of actionable information) ✚ Organize and manage intelligence development process in accordance to relevant requirements ✚ Prepare the data / relevant information for sharing in accordance to relevant
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Advanced knowledge of IT/OT, operating systems and computer networks • Advanced knowledge of cybersecurity solutions • Knowledge of TTP frameworks • Knowledge of big data handling and analytics methods • Knowledge of scripting and programming languages • Advanced knowledge of CTI sharing standards • Knowledge of recent vulnerability disclosures, data breach incidents and geopolitical events impacting cyber risk • Knowledge of advanced and persistent cyber threats and threat actors • Knowledge of statistics and forecasting methodologies	Advanced knowledge of CTI sharing standards Advanced knowledge of IT/OT, operating systems and computer networks Knowledge of advanced and persistent cyber threats and threat actors Knowledge of recent vulnerability disclosures, data breach incidents and geopolitical events impacting cyber risk Knowledge of statistics and forecasting methodologies Knowledge of TTP frameworks Knowledge of scripting and programming languages Knowledge of big data handling and analytics methods ✚ Advanced knowledge of cybersecurity solutions, outputs and integrity to comprehensive cybersecurity concept ✚ Knowledge of data handling techniques ✚ Knowledge of intelligence disciplines, eco-system and methodologies ✚ Knowledge of relevant laws, regulations and industry requirements or guidelines ✚ Knowledge of target methods and procedures

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.		REWIRE	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	B.5. Documentation Production D.7. Data Science and Analytics D.10. Information and Knowledge Management E.4. Relationship Management E.8. Information Security Management	Level 3 Level 4 Level 4 Level 3 Level 4	✚ A.2 Service Level Management ✚ A.7 Technology Trend Monitoring B.5. Documentation Production ✚ B.6. ICT Systems Engineering ✚ D.1. Information Security Strategy Development D.7. Data Science and Analytics D.10. Information and Knowledge Management E.4. Relationship Management E.8. Information Security Management ✚ E.9. Information Systems Governance	Level 4 Level 4 Level 3 Level 3 Level 4 Level 3 Level 4 Level 4 Level 4 Level 4

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.5. CYBERSECURITY ARCHITECT

Table 9: Comparison of ECSF (v.0.5) and REWIRE Cybersecurity architect profile

Source	**ENISA, ECSF, v0.5.**	**REWIRE**
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Solutions Architect Cybersecurity Designer Data Security Architect	✚ Security Architect ✚ Senior Security Architect ✚ Information Security Architect ✚ IT Security Architect ✚ Cyber Security Architect
Summary statement *Indicates the main purpose of the profile.*	Plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls.	
Mission *Describes the rationale of the profile.*	Designs solutions based on security-by-design and privacy-by-design principles. Creates and continuously improves architectural models and develops appropriate architectural documentation and specifications. Coordinate secure development, integration and maintenance of cybersecurity components in line with standards and other related requirements.	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Architecture • Cybersecurity Requirements	
Main task(s) *A list of typical tasks performed by the profile. is tasked to:*	• Design and propose a secure architecture to implement the organisation's strategy • Develop organisation's cybersecurity architecture to address security and privacy requirements • Produce architectural documentation and specifications • Present high-level security architecture design to stakeholders • Establish a secure environment during the development lifecycle of systems, services and products • Coordinate the development, integration and maintenance of cybersecurity components ensuring the cybersecurity specifications • Analyse and evaluate the cybersecurity of the organisation's architecture • Assure the security of the solution architectures through security reviews and certification • Collaborate with other teams and colleagues • Evaluate the impact of cybersecurity solutions on the design and performance of the organisation's architecture • Adapt the organisation's architecture to emerging threats • Assess the implemented architecture to maintain an appropriate level of security	? Analyse and evaluate the organisation's architecture in relation to cybersecurity. ? Assess the implemented architecture against cybersecurity requirements and goals, aiming at the maintainance of an appropriate level of security. ? Collaborate with and advise other teams and colleagues, on the related subjects. ? Design and advise on a secure architecture aligned to the organisation's strategy and the security and privacy requirements. ? Communicate the high-level security architecture design to stakeholders ? Design and implement changes (adaptations) to the organisation's architecture in response to emerging cybersecurity related threats. ? Design and implement security reviews and assessments, support the relevant certification processes and respond to resulting open issues. ? Evaluate the impact of cybersecurity solutions on the design and performance of the organisation's architecture. ? Set up (establish) and manage a suitable environment for the secure development of systems, services and products components, throughout the entire lifecycle.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

		? Document and communicate (as needed) architectural specifications, requirements and other related information. ✚ Manage the development, integration and maintenance of cybersecurity architecture
Key skill(s) *A list of abilities to perform work functions and duties by the profile. Ability to:*	• Conduct user and business requirements analysis • Draw architectural and functional specifications • Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles • Guide and communicate with implementers and IT/OT personnel • Report, communicate and present to stakeholders • Propose cybersecurity architectures based on stakeholder's needs and budget • Select appropriate specifications, procedures and controls • Build resilience against points of failure across the architecture • Provide technological design leadership • Coordinate the integration of security solutions	Conduct user and business requirements analysis Draw architectural and functional specifications Guide and communicate with implementers and IT/OT personnel Report, communicate and present to stakeholders Propose cybersecurity architectures based on stakeholder's needs and budget Select appropriate specifications, procedures and controls Build resilience against points of failure across the architecture Provide technological design leadership Coordinate the integration of security solutions ? Design systems and architectures based on security and privacy by design and by default cybersecurity principles ✚ Analyse the company critical assets and identify weaknesses and vulnerability to intrusion or attack ✚ Assess the extent to which emerging information technologies fit within a given architecture ✚ Assist in communication of the enterprise architecture and standards, principles and objectives to the application teams ✚ Conduct performance and resilience testing ✚ Conduct risk management audits and act to minimise exposures ✚ Contribute to the development of ICT strategy and policy, including ICT security and quality ✚ Define, present and promote an information security policy for approval by the senior management of the organization ✚ Determine requirements for processes related to ICT services ✚ Ensure best architecture solutions are implemented ✚ Keep publications aligned to the solution during the entire lifecycle ✚ Monitor progress of issues throughout lifecycle and communicate effectively ✚ Prepare and conduct tests of ICT systems including automation support ✚ Thinking creatively and innovatively ✚ Understand the business objectives/drivers that impact the architecture component (data, application, security, development etc.) ✚ Working efficiently ✚ Working with digital devices and applications ✚ Collaborating in teams and networks ✚ Dealing with problems ✚ Interpret mathematical information ✚ Planning and organising ✚ Processing information, ideas and concepts

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			✚ Provide expertise to help solve complex technical problems and issues ✚ Report and document tests and results	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Understanding of organisation's mission and business objectives risks • Understanding of security-related standards and requirements • Knowledge of secure development lifecycle • Knowledge of security architecture reference models and security solutions • Knowledge of security technologies and solutions • Knowledge of cybersecurity risks and threats • Knowledge of the latest cybersecurity trends • Understanding of cybersecurity-related standards and compliance requirements • Knowledge of legacy security techniques • Knowledge of Privacy-Enhancing Technologies (PET) • Knowledge of privacy-by-design methodologies		Knowledge of privacy-enhancing technologies (PET). Knowledge of privacy-by-design methodologies Knowledge of legacy security techniques Knowledge of cybersecurity risks and threats Knowledge of secure software development lifecycle \ Knowledge of security architecture reference models and security solutions Knowledge of security technologies and solutions ? Knowledge of security-related standards and requirements ? Knowledge of organisation's mission and business objectives and risks. ? Knowledge of latest cybersecurity trends (new and emerging information technology (IT) and cybersecurity technologies, emerging security issues, threats, vulnerabilities and risks) ? Knowledge of cybersecurity-related standards and compliance requirements ✚ Knowledge of architecture frameworks, methodologies and systems design tools ✚ Knowledge of company's enterprise architecture and its interconnection to networks ✚ Knowledge of costs, benefits and risks of a system architecture ✚ Knowledge of functional & technical designing ✚ Knowledge of information and IT security strategy of the company ✚ Knowledge of information security ✚ Knowledge of key concepts and best practice in asset security ✚ Knowledge of key processes methods and principles to audit and security assessment ✚ Knowledge of organisation's architecture/infastructure ✚ Knowledge of organisation's overall ICT infrastructure and key components ✚ Knowledge of systems development life cycle (best practice design techniques, requirement engineering, technical designing) ✚ Knowledge of standards for documentation, information and content management, documentation reviews and tests	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.5. Architecture Design A.6. Application Design B.1. Application Development B.3. Testing B.6. ICT Systems Engineering	Level 5 Level 3 Level 3 Level 3 Level 4	✚ A.1. IS and Business Strategy Alignment ✚ A.3. Business Plan Development A.5. Architecture Design ✚ A.6. Application Design ✚ A.7. Technology Trend Monitoring B.1. Application Development ✚ B.2. Component Integration	Level 5 Level 4 Level 5 Level 1 Level 4 Level 3 Level 4 Level 3

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			B.3. Testing ✚ B.4. Solution Deployment ✚ B.5. Documentation Production B.6. ICT Systems Engineering ✚ C.4. Problem Management ✚ D.1. Information Security Strategy Development	Level 3 Level 3 Level 4 Level 3 Level 4

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.6. CYBERSECURITY AUDITOR

Table 10: Comparison of ECSF (v.0.5) and REWIRE Cybersecurity auditor profile

Source	**ENISA, ECSF, v0.5.**	**REWIRE**
Alternative Title(s) *Lists titles under the same profile*	Information Security Auditor Cybersecurity Audit Manager Cybersecurity Procedures and Processes Auditor – Source Code Review Auditor Information Security Risk and Compliance Auditor Data Protection Assessment Analyst	✚ Information Security Auditor ✚ Information Security Risk and Compliance Auditor
Summary statement *Indicates the main purpose of the profile.*	Perform cybersecurity audits on the organisation's ecosystem.	
Mission *Describes the rationale of the profile.*	Conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organisation's legal and regulatory frameworks policies. Evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations.	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Audit Plan • Cybersecurity Audit	✚ Cybersecurity Audit documentation
Main task(s) *A list of typical tasks performed by the profile. is tasked to:*	• Develop the organisation's auditing policy, procedures, standards and guidelines • Establish the methodologies and practices used for systems auditing • Establish the target environment and manage auditing activities • Define audit scope, objectives and criteria to audit against • Develop an audit plan describing the frameworks, standards, methodology, procedures and auditing tests • Review target of evaluation, security objectives and requirements based on the risk profile • Audit compliance with cybersecurity-related applicable laws and regulations • Audit conformity with cybersecurity-related applicable standards • Execute the audit plan and collect evidence and measurements • Maintain and protect the integrity of audit records • Develop and communicate conformity assessment, assurance, audit, certification and maintenance reports	? Design and Manage Cybersecurity Audit Policies, Procedures, Standards and guidelines. ? Design methodologies and practices used for cybersecurity audits. ? Define (for each individual audit) the cybersecurity audit scope (including the target environment), objectives and criteria. ? Design, implement, manage, review and update cybersecurity audit plan(s) containing the needed components (frameworks, standards, methodologies, procedures, tests, objectives etc) in alignment with the risk profile(s). ? Perform (Implement) audits against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document audit information and results, in alignment to the relevant audit plan(s). ? Document and communicate the information, evidence, opportunities for improvement, deviations, other information and conclusions of the assessment, audits and tests. ? Maintain and protect the integrity of cybersecurity audit records ✚ Manage cybersecurity audit activities. ✚ Update cybersecurity audit plan(s) including their needed components (frameworks, standards, methodologies, procedures, tests, objectives etc) based on context

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.	REWIRE
		changes (technological landscape, regulations and the organisation's IT assets and technologies). ✚ Support the development and coordination of partnerships with external stakeholders and organisations ✚ Document and communicate opportunities for improvement as a result of assessments, audits and tests.
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Organise and work in a systematic and deterministic way based on evidence • Follow and practice auditing frameworks, standards and methodologies • Apply auditing tools and techniques • Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls • Communicate, explain and adapt legal and regulatory requirements and business needs • Plan and conduct interviews in a systematic and deterministic manner • Collect, evaluate, maintain and protect auditing information • Audit with integrity, being impartial and independent	Organise and work in a systematic and deterministic way based on evidence Follow and practice auditing frameworks, standards and methodologies Apply auditing tools and techniques Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls Communicate, explain and adapt legal and regulatory requirements and business needs Plan and conduct interviews in a systematic and deterministic manner Collect, evaluate, maintain and protect auditing information ✚ Audit with integrity, being impartial and independent ✚ Analyse strategies for critical business functions to ensure plans are within risk mitigation factors ✚ Assess and enhance an organisation's cybersecurity posture, propose effective contingency measures ✚ Assess existing quality standards and align processes and activities with IT product and service quality expectations ✚ Assess risk factors ✚ 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 ✚ Develop and implement standard operating procedures based on IT policies and practices, ensuring compliance with standards and regulations ✚ Develop and test organisational resilience, including techniques for simulations and exercises. ✚ Develop, apply and evaluate algorithms, predictive data modelling and data visualisation to identify underlying trends and patterns in data ✚ Identify and analyse business opportunities ✚ Identify underlying trends and patterns in business data using statistical and computational techniques and tools ✚ Improve related processes. Optimise the series of operations of an organisation to achieve efficiency. Analyse and adapt existing business operations in order to set new objectives and meet new goals. ✚ Manage corrective actions. Implementing corrective action and continuous improvement plans from internal and third party audits to meet cybersecurity performance indicators with adherance to agreed timescales. ✚ Process information, ideas and concepts. Evaluate, input, record, transcribe and update data using electronic or

Source	ENISA, ECSF, v0.5.		REWIRE	
			manual information systems. - processing qualitative information, processing quantitative information, analysing and interpreting information, processing of information ✚ Communicate, present and report ✚ Respect confidentiality obligations. Observe the necessary discretion and restraint when dealing with confidential, secret or unpleasant information. ✚ Review current practices of performing IT-related activities, and propose revisions to security standards and protocols ✚ Use available software features to create and edit documents, customize templates and reports and evaluate online information	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile. (Depending on the level) Basic Understanding of: Understanding of: Knowledge of: Advanced knowledge of:*	• Knowledge of cybersecurity solutions, technical and organisational controls • Knowledge of security controls frameworks, standards • Knowledge of conformity assessment methodologies • Advanced knowledge of auditing frameworks, standards, methodologies and certifications • Knowledge of interviewing techniques		Knowledge of cybersecurity solutions, technical and organisational controls Knowledge of security controls frameworks, standards Knowledge of conformity assessment methodologies Knowledge of auditing frameworks, standards, methodologies and certifications Knowledge of interviewing techniques ✚ Knowledge of business risk management ✚ Knowledge of continuous improvement philosophies, corrective actions processes, and underlying ideas of quality management systems. Implementation process of lean manufacturing, Kanban, Kaizen, Total Quality Management (TQM) and other continuous improvement systems. ✚ Knowledge of costs, benefits and risks of a system architecture ✚ Knowledge of cybersecurity maturity models ✚ Knowledge of cybersecurity risks and threats ✚ Knowledge of ICT internal audit approach ✚ Knowledge of information and IT security strategy of the company ✚ Knowledge of information confidentiality. ✚ Knowledge of project management principles ✚ Knowledge of relevant laws, regulations and industry requirements or guidelines ✚ Knowledge of Root cause analysis (RCA) as a systematic process for identifying root causes of problems or events and an approach for responding to them.	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	– B.3. Testing B.5. Documentation Production E.3. Risk Management E.6 ICT Quality Management E.8. Information Security Management	Level 4 Level 3 Level 4 Level 4 Level 4	✚ A.4 Product/Service Planning B.5. Documentation Production ✚ D.10. Information and Knowledge Management E.3. Risk Management ✚ E.4. Relationship Management E.6 ICT Quality Management E.8. Information Security Management	Level 4 Level 3 Level 4 Level 4 Level 3 Level 4 Level 4

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.7. CYBERSECURITY EDUCATOR

Table 11: Comparison of ECSF (v.0.5) and REWIRE Cybersecurity educator profile

Source	**ENISA, ECSF, v0.5.**	**REWIRE**
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Awareness Specialist Cybersecurity Trainer Professor of Cybersecurity Lecturer in Cybersecurity	✚ Digital Educator ✚ Cyber Instructor
Summary statement *Indicates the main purpose of the profile.*	Improves cybersecurity knowledge, skills and competences of humans.	✚ It should be noted, that this profile contains only the skills, knowledge and e-competences that related to the generic (horizontal) subject of providing education on cybersecurity related topics. In order to provide education on specific cybersecurity domains and topics, the educator should also possess advanced knowledge and where needed experience of those specialized topics.
Mission *Describes the rationale of the profile.*	Designs, develops and conducts awareness, training and educational programmes in cybersecurity and data protection-related topics. Uses appropriate teaching and training methods, techniques and instruments to communicate and enhance the cybersecurity culture, capabilities, knowledge and skills of human resources. Promotes the importance of cybersecurity and consolidates it into the organisation.	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Awareness • Cybersecurity Trainings • Cybersecurity Education	
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need • Organise, design and deliver cybersecurity and data protection awareness-raising activities, seminars, courses, practical training • Monitor, evaluate and report training effectiveness • Evaluate and report trainee's performance • Finding new approaches for education, training and awareness-raising • Design, develop and deliver cybersecurity simulations, virtual labs or cyber range environments • Provide guidance on cybersecurity certification programs for individuals • Continuously maintain and enhance expertise; encourage and empower continuous enhancement of cybersecurity capacities and capabilities building	Continuously maintain and enhance expertise; encourage and empower continuous enhancement of cybersecurity capacities and capabilities building. ? Design, develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need. ? Organise, design and deliver cybersecurity and data protection awareness-raising activities, seminars, courses and practical training to meet relevant needs. ? Monitor, evaluate, document and communicate (as needed) training effectiveness and individual trainee's performance. ? Identify and implement suitable approaches for education, training and awareness-raising based on needs. ? Organise, design and deliver cybersecurity simulations, virtual labs or cyber range environments. ? Advise on cybersecurity skills certification schemes and certificates.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.	REWIRE
		✚ Adapt third party training material to support individual competence development in line with organizational needs. ✚ Perform training needs analyses. ✚ Promote continuous enhancement of cybersecurity capacities and capabilities building.
Key skill(s) *A list of abilities to perform work functions and duties by the profile. Ability to:*	• Identify needs in cybersecurity awareness, training and education – Analyse and deliver cybersecurity education and training • Design, develop and deliver cybersecurity curricula and programmes to meet the organisation and individuals' needs • Develop advanced cybersecurity exercises and scenarios for simulations, virtual or cyber range environments – Provide training towards cybersecurity and data protection professional certifications • Deliver training utilising various training resources • Develop evaluation programs for the awareness, training and education activities • Communicate or author publications, reports, training material • Identify and select appropriate pedagogical approaches for the intended audience • Motivate and incentivise learners	Deliver training utilising various training resources Design, develop and deliver cybersecurity curricula and programmes to meet the organisation and individuals' needs Motivate and incentivize learners Identify and select appropriate pedagogical approaches for the intended audience Develop advanced cybersecurity exercises and scenarios for simulations, virtual or cyber range environments Develop evaluation programs for the awareness, training and education activities Identify needs in cybersecurity awareness, training and education ? Communicate or author publications, reports and training material with the appropriate technical level of documentation ✚ Advise on appropriate solutions in the field of skills certification schemes, taking into consideration the needs of the interested parties ✚ Carry out risk management processes and perform risk analysis to identify required preventive actions and apply mitigation techniques ✚ Communicate in a collaborative environment through different tools ✚ Convey complex information, concepts, or ideas effectively through verbal, written, and/or visual means and to different levels of audience ✚ Gauge learner understanding and knowledge level and, provide effective feedback to students for improving learning ✚ Monitor evolving security and privacy infrastructures, technologies and methods ✚ Plan and organize. Direct activities and tasks, establish schedules and coordinate the activities of groups and individuals to complete objectives on time ✚ Apply critical reading/thinking skills and evaluate information for reliability, validity and relevance ✚ Apply network protection components and security controls ✚ Use cybersecurity techniques, methods and tools for auditing systems and, perform reverse-engineering and forensic analysis
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.*	• Knowledge of pedagogical methods • Advanced knowledge of cybersecurity awareness, education and training programme development • Knowledge of cybersecurity-related professional certifications • Knowledge of cutting-edge methods, tools and techniques	Knowledge of cutting-edge methods, tools and techniques on hands-on cybersecurity education and training Knowledge of cybersecurity frameworks, methodologies, controls and best practices

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Source	ENISA, ECSF, v0.5.		REWIRE	
(Depending on the level) *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	on hands-on cybersecurity education and training • Knowledge of cybersecurity-related legal framework, regulations, standards • Knowledge of cybersecurity frameworks, methodologies, controls and best practices		? Knowledge of pedagogical methods, learning styles and modes of learning ? Knowledge of cybersecurity awareness, education and training programme development ? Knowledge of cybersecurity-related professional certification schemes and certificates ? Knowledge of data protection, data privacy and cyber security-related legislation, policies and regulations ✚ Knowledge of IT technologies and network security methodologies ✚ Knowledge of latest cybersecurity trends (new and emerging information technology (IT) and cybersecurity technologies, emerging security issues, threats, vulnerabilities and risks) ✚ Knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices ✚ Knowledge of tools, techniques and methods for learning assessment and evaluation	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	D.3. Education and Training Provision D.9. Personnel Development E.8. Information Security Management	Level 3 Level 3 Level 3	✚ A.7. Technology Trend Monitoring ✚ B.5. Documentation Production D.3. Education and Training Provision D.9. Personnel Development ✚ E.3. Risk Management E.8. Information Security Management	Level 3 Level 2 Level 3 Level 3 Level 2 Level 3

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.8. CYBERSECURITY IMPLEMENTER

Table 12: Comparison of ECSF (v.0.5) and REWIRE Cybersecurity implementer profile

Source	ENISA, ECSF, v0.5.	REWIRE
Alternative Title(s) *Lists titles under the same profile*	Information Security Implementer Cybersecurity Solutions Expert Cybersecurity Developer Security Engineer Development, Security & Operations (DevSecOps) Engineer	✚ Cyber Defense Infrastructure Support ✚ ICT security specialist ✚ Cybersecurity Engineer ✚ Security Specialist
Summary statement *Indicates the main purpose of the profile.*	Develop, deploy and operate cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products.	
Mission *Describes the rationale of the profile.*	Provides cybersecurity-related technical development, integration, testing, implementation, operation, maintenance, monitoring and support of cybersecurity solutions. Ensures adherence to specifications and conformance requirements, assures sound performance and resolves technical issues required in the organisation's cybersecurity-related solutions (systems, assets, software, controls and services), infrastructures and products.	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Solutions Development • Cybersecurity Solutions Deployment • Cybersecurity Solutions Operation	
Main task(s) *A list of typical tasks performed by the profile. is tasked to:*	• Develop, implement, maintain, upgrade, test cybersecurity products • Provide cybersecurity-related support to users and customers • Integrate cybersecurity solutions and ensure their sound operation • Securely configure systems, services and products • Maintain and upgrade the security of systems, services and products • Implement cybersecurity procedures and controls • Monitor and assure the performance of the implemented cybersecurity controls • Document and report on the security of systems, services and products • Work close with the IT/OT personnel on cybersecurity-related actions • Implement, apply and manage patches to products to address technical vulnerabilities	Securely configure systems, services and products. Integrate cybersecurity solutions and ensure their sound operation. Implement cybersecurity procedures and controls. ? Implement, customize, operate, maintain, upgrade and test cybersecurity products. ? Document information and results related to the security of systems, services and products. Communicate as needed. ? Support users and other related parties as needed on cybersecurity-related issues. ? Identify, plan, implement, apply and manage patches to products to address technical vulnerabilities. Respond to issues by implementing required actions as needed. ? Monitor, assess, evaluate and assure the performance of the implemented cybersecurity controls. ? Collaborate with the IT/OT personnel on cybersecurity-related actions.
Key skill(s) *A list of abilities to perform work functions and*	• Document, report present and communicate with various stakeholders • Integrate cybersecurity solutions to the organisation's infrastructure	Assess the security and performance of solutions Configure solutions according to the organisation's security policy Develop and test secure code and scripts

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

duties by the profile. Ability to:	• Configure solutions according to the organisation's security policy • Assess the security and performance of solutions • Develop and test secure code and scripts • Identify and troubleshoot cybersecurity-related issues • Collaborate with other team members and colleagues	Identify, troubleshoot and respond to cybersecurity-related issues Integrate cybersecurity solutions to the organisation's infrastructure Collaborate with other team members and colleagues ? Communicate, present and report relevant information with and to various stakeholders ✚ Clearly communicate with users and other parties and provide instructions on how to progress issues ✚ Analyse symptoms to identify broad area of user error or technical failure ✚ Communicate effectively to ensure appropriate resources are deployed internally or externally to minimize outages ✚ Contribute to the identification of risks that arise from potential technical solution architectures. Suggest alternate solutions or countermeasures to mitigate risks. Define secure systems configurations in compliance with intended architectures ✚ Deploy support tools to systematically trace source of error or technical failure ✚ Develop and implement solutions to practical, operational or conceptual problems which arise in the execution of work, in a wide range of contexts ✚ Operate, maintain, monitor, document and assure the performance of the implemented cybersecurity controls ✚ Performs basic risk assessments for small information systems. ✚ Protect devices and digital content, and understand risks and threats in digital environments. Make use of tools and methods which maximise security of ICT devices and information by controlling access, such as passwords, digital signatures, biometry, and protecting systems such as firewall, antivirus, spam filters. ✚ Research, understand, act up on, resolve security vulnerabilities
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of systems development life cycle • Knowledge of programming languages • Knowledge of operating systems security • Knowledge of computer networks security • Knowledge of security controls • Knowledge of offensive and defensive security practices • Knowledge of secure coding practices • Knowledge of test methodologies and practices	Knowledge of offensive and defensive security practices ? Knowledge of security controls (principles and techniques for access management, principles of systems and data security, web, cloud and mobile technologies and conditions for effective and secure implementation) ? Knowledge of scripting and programming languages ? Knowledge of operating systems security (database management systems, Operating Systems and software platforms (including managed services and APIs) ? Knowledge of secure coding practices (development tools (e.g. development environment, management, source code access/revision control), known vulnerabilities and secure code/component libraries ? Knowledge of systems development life cycle (best practice design techniques, requirement engineering, technical designing) ? Knowledge of test methodologies and practices (integration testing techniques, techniques, infrastructure and tools to be used in the testing process, the lifecycle of a testing process)

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			? Knowledge of computer networks security (including. loT. LAN. WLAN, mobile. Bluetooth, components, topologies, protocols, interconnections, B6K6 cloud and platform business models like SaaS. PaaS. laaS) ✚ Knowledge of different sorts of tests (functional, integration, performance, usability, accessibility, security, stress etc.), national and international standards defining quality criteria for testing, testing methods, tools and automation including agile approaches, vulnerability and misuse testing ✚ Knowledge of incident management processes, handling methodologies, best practices and terminology ✚ Knowledge of system administration, network, and operating system hardening techniques ✚ Knowledge of risk management terms (principles, models, methods, tools and techniques of risk management and risk analysis, economics of security & risk management) ✚ Knowledge of OSI model, underlying network protocols (e.g., TCP/IP), Dynamic Host Configuration, Domain Name System (DNS), and directory services ✚ Knowledge of asset management (hardware components, tools and architectures, physical devices like sensors, actors, the organisation's overall ICT /OT infrastructure and key components, key concepts and best practice in asset security)	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofess ionalism.org/explorer*	A.7. Technology Trend Monitoring B.2. Component Integration B.3. Testing B.5. Documentation Production C.4. Problem Management	Level 3 Level 2 Level 3 Level 3 Level 4	✚ A.5. Architecture Design A.7. Technology Trend Monitoring B.2. Component Integration B.3. Testing ✚ B.4. Solution Deployment B.5. Documentation Production ✚ B.6. ICT Systems Engineering ✚ C.1. User Support C.4. Problem Management ✚ C.5. Systems Management ✚ D.1. Information Security Strategy Development ✚ E.3. Risk Management ✚ E.8. Information Security Management	Level 3 Level 3 Level 3 Level 3 Level 3 Level 2 Level 4 Level 2 Level 3 Level 3 Level 4 Level 2 Level 3

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.9. CYBERSECURITY RESEARCHER

Table 13: Comparison of ECSF (v.0.5) and REWIRE Cybersecurity researcher profile

Source	**ENISA, ECSF, v0.5.**	**REWIRE**
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Research Engineer Chief Research Officer (CRO) in cybersecurity Senior Research Officer in cybersecurity Research and Development (R&D) Officer in cybersecurity Scientific Staff in cybersecurity Research and Innovation Officer/Expert in cybersecurity Research Fellow in cybersecurity	
Summary statement *Indicates the main purpose of the profile.*	Research the cybersecurity domain and incorporate results in cybersecurity solutions.	
Mission *Describes the rationale of the profile.*	Conducts fundamental/basic and applied research and facilitates innovation in the cybersecurity domain through cooperation with other stakeholders. Analyses trends and scientific findings in cybersecurity.	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Research in Cybersecurity	
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	Analyse and assess cybersecurity technologies, solutions, developments and processes Advance the current state-of-the-art in cybersecurity-related topics Assist in cybersecurity-related capacity building including awareness, theoretical training, practical training, testing, mentoring, supervising and sharing Assist in the development of innovative cybersecurity-related solutions Conduct experiments and develop a proof of concept, pilots and prototypes for cybersecurity solutions Conduct research, innovation and development work in cybersecurity-related topics Contributes towards cutting-edge cybersecurity business ideas, services and solutions Identify cross-sectoral cybersecurity achievements and apply them in a different context or propose innovative approaches and solutions Lead or participate in the innovation processes and projects including project management and budgeting Manifest and generate research and innovation ideas Publish and present scientific works and research and development results	Conduct experiments and develop proof of concept(s), pilot(s) and prototypes for cybersecurity solution. Conduct research, innovation and development work in cybersecurity-related topics. Lead or participate in the innovation processes and projects including project management and budgeting. ✚ Collaborate and communicate with stakeholders to identify and/or develop appropriate solutions technology. ✚ Design, develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need. ? Develop innovative cybersecurity-related solutions (in total or partially). ? Identify, analyse and assess cybersecurity technologies, solutions, developments and processes. ? Identify, conseptualize and generate research and innovation ideas, to advance the current state-of-the-art in cybersecurity-related topics. ? Organise, design and deliver cybersecurity and data protection awareness-raising activities, seminars, courses and practical training

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	Select and apply frameworks, methods, standards, tools and protocols including a building and testing a proof of concept to support projects		to meet needs. Participate in mentoring, supervision and sharing activities as needed. ? Design, develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need. ? Design, develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need. ? Design, develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need.	
Key skill(s) *A list of abilities to perform work functions and duties by the profile. Ability to:*	• Generate new ideas and transfer theory into practice • Decompose, analyse systems, spot weaknesses, develop security and privacy requirements and identify effective or ineffective related solutions • Analyse and solve complex problems and security challenges • Continuously monitor new advancements and cybersecurity innovations • Communicate and disseminate the scientific outcomes • Prove the soundness of the research results • Collaborate with other team members		Generate new ideas and transfer theory into practice Decompose, analyse systems, spot weaknesses, develop security and privacy requirements and identify effective or ineffective related solutions Analyse and solve complex problems and security challenges Communicate and disseminate the scientific outcomes Continuously monitor new advancements and cybersecurity innovations Prove the soundness of the research results ? Work in a team and cooperate with colleagues and different external partners ✚ Communicate, present and report ✚ Thinking creatively and innovatively	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile. (Depending on the level) Basic Understanding of: Understanding of: Knowledge of: Advanced knowledge of:*	Knowledge of cybersecurity methods, methodologies, tools and techniques Knowledge of programs and grants Knowledge of project management and budgeting Knowledge of research, development and innovation (RDI) relevant to cybersecurity subject matters Understanding of copyright and intellectual property rights issues, standards and patent filing Understanding of espionage and coercion threats and risk in international research Understanding of responsible disclosure of cybersecurity-related information Understanding of the multidiscipline aspect of cybersecurity		Knowledge of cybersecurity methods, methodologies, tools and techniques Knowledge of research, development and innovation (RDI) relevant to cybersecurity subject matters Knowledge of responsible disclosure of cybersecurity-related information ? Knowledge of copyright and intellectual property rights issues, standards and patent filing ? Knowledge of data protection, data privacy, cyber security-related legislation, policies and regulations ? Knowledge of espionage and coercion threats and risks ? Knowledge of funding programs and grants ? Knowledge of multidiscipline aspect of cybersecurity ? Knowledge of project management and budgeting, risk management ✚ Knowledge of ethical issues, rules and constraints	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.7. Technology Trend Monitoring A.9. Innovating D.7. Data Science and Analytics C.4. Problem Management D.10. Information and Knowledge Management	Level 5 Level 5 Level 4 Level 3 Level 3	✚ A.6. Application Design A.7. Technology Trend Monitoring A.9. Innovating ✚ B.1. Application Development ✚ B.3. Testing C.4. Problem Management ✚ D.4. Education and Training Provision ✚ D.7. Data Science and Analytics D.10. Information and Knowledge Management ✚ E.3. Risk Management	Level 2 Level 5 Level 5 Level 2 Level 2 Level 3 Level 2 Level 4 Level 3 Level 2

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.10. CYBERSECURITY RISK MANAGER

Table 14: Comparison of ECSF (v.0.5) and REWIRE Cybersecurity risk manager profile

Source	ENISA, ECSF, v0.5.	REWIRE
Alternative Title(s) *Lists titles under the same profile*	– Information Security Risk Analyst Cybersecurity Risk Assurance Consultant Cybersecurity Risk Assessor – Cybersecurity Impact Analyst	✚ Cyber Risk Manager ✚ Information Security Risk Manager
Summary statement *Indicates the main purpose of the profile.*	Manage the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop, maintain and communicate the risk management processes and reports.	? Identify the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop Organization's Risk management framework. Develop, maintain, and communicate the risk management processes and reports. Use models like eg. RACI to explicitly define the roles of stakeholders within the Organization's Risk Management Framework (RMF).
Mission *Describes the rationale of the profile.*	Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organisation and ensures that risks remain at an acceptable level for the organisation by selecting mitigation actions and controls.	? Continuously identifies, analyses, assesses, calculates and proposes mitigation actions. ? The cybersecurity-related risks of ICT infrastructures, systems services, and assets by planning, applying, reporting and communicating risk analysis, assessment and treatment. ? Establishes a risk management strategy for the organisation and ensures that risks owners and Risk Committee are aware of the current cybersecurity-related risks that the Organization is exposed to. ✚ Establish policies for cybersecurity risk management that include roles and responsibilities. ✚ Communicate with internal and external stakeholders. ✚ Reporting to Risk Committees and Regulators / Authorities e.g. Central Banks, Commissioners, Digital Security Authorities. ✚ Involved in the security by design framework.
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Risk Management	
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy Develop an organisation's cybersecurity risk management strategy Develop, maintain, report and communicate complete risk management cycle – Ensure that all cybersecurity risks remain at an acceptable level for the organisation's assets Identification of threat landscape including attackers' profiles and estimation of attacks' potential – Manage an inventory of organisation's assets	? Assess cybersecurity risks and advise on appropriate risk treatment options in alignment with the business strategy and objectives. ? Design, develop and manage the organization's cybersecurity risk management strategy in alignment with the business strategy to support the organizational objectives. ? Design, develop, implement and manage cybersecurity risk management policies, processes, procedures, standards, guidelines and frameworks (including roles and responsibilities). ? Identify and analyze the threat landscape (including attackers' profiles and estimation of attacks' potential). ? Identify, analyze and assess cybersecurity-related threats and vulnerabilities.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems Monitor effectiveness of cybersecurity controls and risk levels	? Monitor, measure and evaluate the effectiveness of implemented cybersecurity controls and risk levels. ✚ Advise different functions internally on cybersecurity risks, methodologies, tools, updates, threat scenarios, etc. ✚ Communicate cybersecurity related risks, issues, updates, processes and actions internally as needed. ✚ Communicate with internal and external stakeholders to ensure appropriate resources are deployed internally or externally to support the risk management process. ✚ Document the information and results of the Risk Management process and individual activities.
Key skill(s) *A list of abilities to perform work functions and duties by the profile. Ability to:*	• Analyse and consolidate organisation's quality and risk management practices • Build a cybersecurity risk-aware environment • Communicate, present and report to relevant stakeholders • Enable business assets owners, executives and other stakeholders to make risk informed decisions to manage and mitigate risks • Enable employees to understand, embrace and follow the controls • Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards • Propose and manage risk-sharing options	Analyse and consolidate organisation's quality and risk management practices Build a cybersecurity risk-aware environment Propose and manage risk-sharing options Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards Enable employees to understand, embrace and follow the controls Enable business assets owners, executives and other stakeholders to make risk informed decisions to manage and mitigate risks Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards ? Communicate, present and report ✚ Analyze and consolidate organisation's quality and risk management practices ✚ Apply risk management processes, identify risks and apply a risk management process. ✚ Identify sources of information that can be used for monitoring and measurement of cybersecurity controls. ✚ Interpret the results, reports of vulnerability assessments and penetration tests ✚ Oversee and control the implementation of prevention, security, and surveillance measures in order to assess their effectiveness and to make adjustments in case of unsatisfactory results. ✚ Use monitoring tools to measure and evaluate the effectiveness of implemented cybersecurity controls and the achieved security levels.
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile. (Depending on the level) Basic Understanding of: Understanding of: Knowledge of: Advanced knowledge of:*	• Advanced knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices • Knowledge of cyber threats, threats taxonomies and vulnerabilities repositories • Knowledge of risk sharing options and best practices • Knowledge of technical and organisational controls that appropriately mitigate cybersecurity risks • Knowledge of cybersecurity-related technologies and controls • Knowledge of monitoring, implementing, testing and evaluating the effectiveness of the controls	? Knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices ? Knowledge of cybersecurity threats, vulnerabilities and risks (threats taxonomies and vulnerabilities repositories) Knowledge of technical and organisational controls that appropriately mitigate cybersecurity risks Knowledge of risk sharing options and best practices Knowledge of cybersecurity-related technologies and controls Knowledge of monitoring, implementing, testing and evaluating the effectiveness of the controls

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	B.5. Documentation Production E.3. Risk Management – E.5. Process Improvement – E.7. Business Change Management E.9. IS-Governance	Level 3 Level 4 Level 3 Level 4 Level 4	? B.5. Documentation Production ✚ B.2. Component Integration ✚ D.1. Information Security Strategy Development ✚ D.7. Data Science and Analytics ✚ D.10. Information and Knowledge Management ✚ E.8. Information Security Management E.3. Risk Management E.9. IS-Governance	Level 2 Level 4 Level 5 Level 4 Level 4 Level 3 Level 4 Level 4

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.11. DIGITAL FORENSICS INVESTIGATOR

Table 15: Comparison of ECSF (v.0.5) and REWIRE Digital forensics investigator profile

Source	ENISA, ECSF, v0.5.	REWIRE
Alternative Title(s) *Lists titles under the same profile*	Digital Forensics Analyst Cybersecurity & Forensic Specialist Computer Forensics Consultant	✚ Incident responder ✚ Security Incident Response Engineer ✚ Malware analyst ✚ CTI analyst
Summary statement *Indicates the main purpose of the profile.*	Ensure the cybercriminal investigation reveals all digital evidence to prove the malicious activity.	
Mission *Describes the rationale of the profile.*	Connects artefacts to natural persons, captures, recovers, identifies and preserves data, including manifestations, inputs, outputs and processes of digital systems under investigation. Provides analysis, reconstruction and interpretation of the digital evidence based on a qualitative opinion. Presents an unbiased qualitative view without interpreting the resultant findings.	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Digital Forensics Analysis	
Main task(s) *A list of typical tasks performed by the profile. is tasked to:*	• Develop digital forensics investigation policy, plans and procedures • Identify, recover, extract, document and analyse digital evidence • Preserve and protect digital evidence and make it available to authorized stakeholders • Inspect environments for evidence of unauthorised and unlawful actions • Systematically and deterministic document, report and present digital forensic analysis findings and results • Select and customise forensics testing, analysing and reporting techniques	✚ Analyze hardware components ✚ Monitor external data sources (e.g., Computer Emergency Response Teams, Security Focus,) and maintain currency of knowledge on the relevant legislation, regulations, methods, techniques etc. ✚ Advise internal stakeholders on how to secure and preserve digital evidence and the relevant constraints and processes. ? Identify, select and customise (as needed) forensics testing, analysing and reporting techniques ? Document, report and communicate digital forensic analysis findings and results in a systematic, professional and deterministic manner. ? Design, develop, implement and manage digital forensics investigation policies, processes, procedures, standards, guidelines and plans. Inspect environments for evidence of unauthorised and unlawful actions. Identify, recover, extract, document and analyse digital evidence. Preserve and protect digital evidence and make it available to authorized stakeholders.
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Collect information while preserving its integrity • Develop and communicate, detailed and reasoned investigation reports	Collect information while preserving its integrity Explain and present digital evidence in a simple, straightforward and easy to understand way ? Develop and follow leads to assess evidence creatively

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	• Explain and present digital evidence in a simple, straightforward and easy to understand way • Identify, analyse and correlate events • Work ethically and independently; not influenced and biased by internal or external actors		? Develop detailed and reasoned investigation reports ✚ Communicate, present and report ✚ Strictly and systematically follow the prescribed procedures. ✚ Use specific tools, techniques and methods in relation to digital forensics (extracting, reversing and understanding code and traces, logs, malware analysis, protocols, operating systems, etc) ✚ Work ethically, following codes of professional ethics or other equivalent ✚ Recognize and categorize types of vulnerabilities and associated attacks ✚ Manage Information sources. Identify relevant internal and external information sources and providers. Organise the information workflow and define information deliverables ✚ Assess Information needs. Communicate with stakeholders in order to identify which information is required and the methods with which it can be accessed ✚ Define digital forensics inversigation policies and other documentation. Specify policies, principles, rules, processes and criteria for the design, planning and realisations related to digital forensics inversigation.	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Advanced knowledge of cybersecurity attacks tactics and techniques • Knowledge of criminal investigation methodologies and procedures • Knowledge of cyber threats and vulnerabilities • Knowledge of digital forensics analysis techniques • Knowledge of digital forensics methods, best practices and tools • Knowledge of digital forensics testing techniques • Knowledge of legal framework related to cybersecurity and data protection • Knowledge of malware analysis tools • Knowledge of operating systems internals, networking protocols and services		✚ Knowledge of application protocols and services ✚ Knowledge of assembly and low-level programming interfaces ✚ Knowledge of ethical issues, rules and constraints regarding forensics investigation ✚ Knowledge of legal framework for digital evidence creation and conservation ✚ Knowledge of network environments, including field buses ✚ Knowledge of scripting and programming languages ✚ Knowledge of TCP/IP networking ✚ Knowledge of ATT&CK patterns Knowledge of criminal investigation methodologies and procedures Knowledge of cyber threats and vulnerabilities Knowledge of malware analysis tools ? Knowledge of digital forensics analysis and testing techniques, best practices and tools (extracting, reversing and understanding code and traces, logs) ? Knowledge of data protection, data privacy, cyber security-related legislation, policies and regulations ? Knowledge of operating systems, networking protocols and services ? Knowledge of offensive and defensive security practices	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.7. Technology Trend Monitoring B.3. Testing B.5. Documentation Production E.3. Risk Management	Level 3 Level 4 Level 3 Level 3	A.7. Technology Trend Monitoring B.3. Testing B.5. Documentation Production ✚ D.10. Information and Knowledge Management E.3. Risk Management ✚ E.8. Information Security Management	Level 3 Level 4 Level 3 Level 4 Level 3 Level 3

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.12. PENETRATION TESTER

Table 14: Comparison of ECSF (v.0.5) and REWIRE Penetration tester profile

Source	ENISA, ECSF, v0.5.	REWIRE
Alternative Title(s) *Lists titles under the same profile*	Pentester Ethical Hacker Vulnerability Analyst Cybersecurity Tester Offensive Cybersecurity Expert – Defensive Cybersecurity Expert Red Team Expert	? Red Teamer
Summary statement *Indicates the main purpose of the profile.*	Assess the effectiveness of security controls, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors.	
Mission *Describes the rationale of the profile.*	Plans, designs, implements and executes penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures. Identifies vulnerabilities or failures on technical and organisational controls that affect the confidentiality, integrity and availability of ICT products (e.g. systems, hardware, software and services).	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Technical Cybersecurity Assessment	
Main task(s) *A list of typical tasks performed by the profile. is tasked to:*	• Deploy penetration testing tools and test programs • Document and report penetration testing results to stakeholders • Establish procedures for penetration testing result analysis and reporting • Identify attack vectors, uncover, and demonstrate exploitation of technical cybersecurity vulnerabilities • Identify, analyse, and assess technical and organisational cybersecurity vulnerabilities • Organise test plans and procedures for penetration testing • Select and develop appropriate penetration testing techniques • Test systems and operations compliance with regulatory standards	Identify attack vectors, uncover and demonstrate exploitation of technical cybersecurity vulnerabilities. Identify, analyse and assess technical and organisational cybersecurity vulnerabilities. ✚ Advise and support internal stakeholders on subjects related to penetration testing. ? Document and communicate penetration testing results to stakeholders as needed. Classify findings, propose mitigation actions and re-test as needed. ? Identify, select, develop and customize appropriate penetration testing techniques. ? Design, develop, implement and manage test plans and procedures for penetration testing (including result analysis and reporting). ? Install, customize, operate, maintain and upgrade testing tools (platforms, hardware and software). ? Perform (Implement) tests against cybersecurity-related applicable laws, regulations and standards, collect needed evidence and document test information and

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			results, in alignment to the relevant test plan(s).	
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Adapt and customise penetration testing tools and techniques • Communicate and report • Conduct ethical hacking • Develop codes, scripts and programmes • Identify and exploit vulnerabilities • Perform social engineering • Solve and troubleshoot problems • Think creatively and outside the box • Use penetration testing tools effectively		Adapt and customise penetration testing tools and techniques Conduct ethical hacking Develop codes, scripts and programmes Identify and exploit vulnerabilities Solve and troubleshoot problems Use penetration testing tools effectively ? Apply social engineering techniques ? Communicate, present and report ? Thinking creatively and innovatively ✚ Assess cybersecurity vulnerabilities ✚ Explain and communicate technical cybersecurity topics appropriately to a variety of stakeholders.	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	Advanced knowledge of cybersecurity attack vectors Advanced knowledge of IT/OT appliances, operating systems and computer networks Advanced knowledge of penetration testing tools, techniques and methodologies Knowledge of best practices on cybersecurity Knowledge of scripting and programming languages Knowledge of security vulnerabilities		? Knowledge cybersecurity attack vectors ? Knowledge of IT/OT appliances, operating systems and computer networks ? Knowledge of penetration testing tools, techniques and methodologies Knowledge of scripting and programming languages ✚ Knowledge of ethical issues, rules and constraints ✚ Knowledge of offensive and defensive security practices ✚ Knowledge of cybersecurity threats, vulnerabilities and risks ✚ Knowledge of relevant laws, regulations and industry standards	
e-Competences (from e-CF) For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer	B.2. Component Integration B.3. Testing B.4. Solution Deployment B.5. Documentation Production E.3. Risk Management	Level 4 Level 4 Level 2 Level 3 Level 4	B.2. Component Integration B.3. Testing B.4. Solution Deployment B.5. Documentation Production E.3. Risk Management	Level 4 Level 4 Level 2 Level 3 Level 4

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CONCLUSIONS

This document provides an analysis and extension of the ENISA's ECSF v0.5, currently under review. It analyzes and extends the skills proposed by ENISA with content from other frameworks or relevant tools, to provide more extensive job profiles.

For each one of 12 ENISA roles profiles, the same, similar, or close matches were identified to the frameworks and other sources such as the Cybersecurity Skills Framework of Singapore, ASD Cyber skills framework, the European ICT Professional Role Profiles, European e-Competence Framework (e-CF), SFIA Skills Framework for the Information Age and National Initiative for Cybersecurity Education. The REWIRE team also consulted the Cyberseek and Cyber Career Pathways Tool developed based on the NIST NICE framework, ESCO framework, and the ECHO Cyberskills Framework. The findings of Job analyser were considered as well.

Each one of the ENISA roles profiles was enhanced by the tasks, knowledge, skills, and competences that were missing. Possible alternative titles were added as well. To ensure the use of the same language for the same knowledge, all profiles were deconstructed, and one list of tasks, skills and knowledge was established. It was revised linguistically and content-wise to ensure that the same language was used in all the role profiles. Competences, skills, and knowledge were combined with the tasks attached to a particular role profile and compared to ECSF v0.5.

To facilitate the market needs, it is recommended that the profiles are split into three categories / levels: Junior, Middle, Senior; for each level the relevant skills, knowledge, e-competences and other expertise are identified and aligned.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

REFERENCES

[i] European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf, accessed on 2022-08-23

[ii] Cyber security competence for research and innovation (CONCORDIA). https://www.concordia-h2020.eu, accessed on 2022-08-23

[iii] European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO). https://echonetwork.eu, accessed on 2022-08-23

[iv] Cyber security for Europe (CyberSec4Europe). https://cybersec4europe.eu, accessed on 2022-08-23

[v] Strategic programs for advanced research and technology in Europe (SPARTA). https://www.sparta.eu, accessed on 2022-08-23

[vi] ENISA. Cybersecurity skills - Building a cybersecurity workforce. https://www.enisa.europa.eu/events/cybersecurity-skills-building-a-cybersecurity-workforce

[vii] ENISA. European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[viii] ENISA. European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[ix] ENISA. European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[x] ENISA. Ad-Hoc Working Group on the European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

[xi] ENISA. European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[xii] On April 5, 2022, a consolidated draft version of the European Cybersecurity Skills Framework was presented to the public through a webinar, during which the framework structure and benefits were presented, along with various use cases. https://www.youtube.com/watch?v=yTuWWg_JG64, accessed on 2022-08-23

[xiii] CEN. (2018). CWA 16458-1:2018 European ICT Professional Role Profiles – Part 1: 30 ICT Profiles. Geneva: CEN, CEN. (2018). CWA 16458-3:2018, European ICT professional role profiles - Part 3: Methodology documentation. https://www.ecompetences.eu/ict-professional-profiles, , accessed on 2022-08-23

[xiv] NIST. (2018). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf, accessed on 2022-08-23

[xv] CEN/TC 428. (2020)

[xvi] NIST. (2018). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf, , accessed on 2022-08-23

[xvii] CEN. (2018). CWA 16458-1:2018 European ICT Professional Role Profiles – Part 1: 30 ICT Profiles. Geneva: CEN, CEN. (2018). CWA 16458-3:2018, European ICT professional role profiles - Part 3: Methodology documentation. https://www.ecompetences.eu/ict-professional-profiles, accessed on 2022-08-23

[xviii] NIST. (2018). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf, accessed on 2022-08-23

[xix] CEN/TC 428. (2020)

[xx] The e-Competence Framework. https://itprofessionalism.org/about-it-professionalism/competences/the-e-competence-framework, accessed on 2022-08-23

[xxi] CEN CWA 16458-1:2018, European ICT professionals role profiles – Part 1: 30 ICT profiles

[xxii] https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html, accessed on 2022-08-23

[xxiii] Australian Government, Australian Signals Directorate, ASD Cyber Skills Framework: https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf, accessed on 2022-08-23

[xxiv] Australian Government, Australian Signals Directorate, ASD Cyber Skills Framework: https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf, accessed on 2022-08-23

[xxv] The European ICT Professional Role Profiles, https://itprofessionalism.org/about-it-professionalism/competences/ict-profiles/, accessed on 2022-08-23

[xxvi] The European ICT Professional Role Profiles, https://itprofessionalism.org/about-it-professionalism/competences/ict-profiles/, accessed on 2022-08-23

[xxvii] Workforce Framework for Cybersecurity (NICE Framework), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf, accessed on 2022-08-23

[xxviii] D2.6 ECHO CYBERSKILLS FRAMEWORK, https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf, accessed on 2022-08-23

[xxix] SFIA VIEW: SFIA FULL FRAMEWORK VIEW, https://sfia-online.org/en/legacy-sfia/sfia-7/sfia-views/full-framework-view?path=/glance, accessed on 2022-08-23

[xxx] HSD job profiles and their analysis, https://securitytalent.nl/career/job-profiles, accessed on 2022-08-23

[xxxi] HSD interactive career map tool, https://securitytalent.nl/career/career-navigator-in-safety-security, accessed on 2022-08-23

[xxxii] Cyberseek tool - CYBERSECURITY CAREER PATHWAY, https://www.cyberseek.org/pathway.html, accessed on 2022-08-23

[xxxiii] Cyber Career Pathways Tool, https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool, accessed on 2022-08-23

[xxxiv] ESCO (European Skills, Competences, Qualifications and Occupations) Occupations, https://esco.ec.europa.eu/en/classification/occupation_main, accessed on 2022-08-23

[xxxv] https://dictionary.cambridge.org/dictionary/english/advise

[xxxvi] https://dictionary.cambridge.org/dictionary/english/analyse

[xxxvii] https://dictionary.cambridge.org/dictionary/english/assess?q=ASSESS

[xxxviii] https://dictionary.cambridge.org/dictionary/english/assist

[xxxix] ISO 9000:2015(en), Quality management systems — Fundamentals and vocabulary

[xl] https://dictionary.cambridge.org/dictionary/english/communicate

[xli] (ISO 9000:2015(en), Quality management systems — Fundamentals and vocabulary)

[xlii] https://dictionary.cambridge.org/dictionary/english/develop

[xliii] https://dictionary.cambridge.org/dictionary/english/document

[xliv] https://dictionary.cambridge.org/dictionary/english/evaluate

[xlv] https://dictionary.cambridge.org/dictionary/english/identify

[xlvi] https://dictionary.cambridge.org/dictionary/english/implement

[xlvii] (ISO 9000:2015(en), Quality management systems — Fundamentals and vocabulary)

[xlviii] https://dictionary.cambridge.org/dictionary/english/support

[xlix] (ISO 9000:2015(en), Quality management systems — Fundamentals and vocabulary)

[l] https://dictionary.cambridge.org/dictionary/english/train

[li] https://dictionary.cambridge.org/dictionary/english/advise

[lii] https://dictionary.cambridge.org/dictionary/english/adapt

[liii] https://dictionary.cambridge.org/dictionary/english/align

[liv] https://dictionary.cambridge.org/dictionary/english/analyse

[lv] https://dictionary.cambridge.org/dictionary/english/anticipate

[lvi] https://dictionary.cambridge.org/dictionary/english/apply

[lvii] https://dictionary.cambridge.org/dictionary/english/automate

[lviii] https://dictionary.cambridge.org/dictionary/english/author

[lix] https://dictionary.cambridge.org/dictionary/english/assess?q=ASSESS

[lx] https://dictionary.cambridge.org/dictionary/english/assist

[lxi] ISO 9000:2015(en), Quality management systems — Fundamentals and vocabulary

[lxii] https://dictionary.cambridge.org/dictionary/english/build

[lxiii] https://dictionary.cambridge.org/dictionary/english/capture

[lxiv] https://dictionary.cambridge.org/dictionary/english/categorize?q=categorise

[lxv] https://dictionary.cambridge.org/dictionary/english/communicate

[lxvi] https://dictionary.cambridge.org/dictionary/english/configure

[lxvii] https://dictionary.cambridge.org/dictionary/english/conduct

[lxviii] https://dictionary.cambridge.org/dictionary/english/convey

[lxix] https://dictionary.cambridge.org/dictionary/english/contribute

[lxx] https://dictionary.cambridge.org/dictionary/english/coordinate

[lxxi] https://dictionary.cambridge.org/dictionary/english/cooperate

[lxxii] https://dictionary.cambridge.org/dictionary/english/correlate

[lxxiii] https://dictionary.cambridge.org/dictionary/english/define

[lxxiv] https://dictionary.cambridge.org/dictionary/english/deliver

[lxxv] (ISO 9000:2015(en), Quality management systems — Fundamentals and vocabulary)

[lxxvi] https://dictionary.cambridge.org/dictionary/english/determine

[lxxvii] https://dictionary.cambridge.org/dictionary/english/develop

[lxxviii] https://dictionary.cambridge.org/dictionary/english/direct

[lxxix] https://dictionary.cambridge.org/dictionary/english/disseminate

[lxxx] https://dictionary.cambridge.org/dictionary/english/document

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

[lxxxi] https://dictionary.cambridge.org/dictionary/english/enable

[lxxxii] https://dictionary.cambridge.org/dictionary/english/enhance

[lxxxiii] https://dictionary.cambridge.org/dictionary/english/ensure

[lxxxiv] https://dictionary.cambridge.org/dictionary/english/establish

[lxxxv] https://dictionary.cambridge.org/dictionary/english/evaluate

[lxxxvi] https://dictionary.cambridge.org/dictionary/english/explain

[lxxxvii] https://dictionary.cambridge.org/dictionary/english/follow

[lxxxviii] https://dictionary.cambridge.org/dictionary/english/gauge

[lxxxix] https://dictionary.cambridge.org/dictionary/english/guide

[xc] https://dictionary.cambridge.org/dictionary/english/identify

[xci] https://dictionary.cambridge.org/dictionary/english/implement

[xcii] https://dictionary.cambridge.org/dictionary/english/improve

[xciii] https://dictionary.cambridge.org/dictionary/english/incentivize?q=Incentivize

[xciv] https://dictionary.cambridge.org/dictionary/english/influence

[xcv] https://dictionary.cambridge.org/dictionary/english/integrate

[xcvi] https://dictionary.cambridge.org/dictionary/english/interpret

[xcvii] https://dictionary.cambridge.org/dictionary/english/lead

[xcviii] (ISO 9000:2015(en), Quality management systems — Fundamentals and vocabulary)

[xcix] https://dictionary.cambridge.org/dictionary/english/maintain

[c] https://dictionary.cambridge.org/dictionary/english/operate

[ci] https://dictionary.cambridge.org/dictionary/english/organize

[cii] https://dictionary.cambridge.org/dictionary/english/perform

[ciii] https://dictionary.cambridge.org/dictionary/english/plan

[civ] https://dictionary.cambridge.org/dictionary/english/practice

[cv] https://dictionary.cambridge.org/dictionary/english/prepare

[cvi] https://dictionary.cambridge.org/dictionary/english/preserve

[cvii] https://dictionary.cambridge.org/dictionary/english/promote

[cviii] https://dictionary.cambridge.org/dictionary/english/propose

[cix] https://dictionary.cambridge.org/dictionary/english/protect

[cx] https://dictionary.cambridge.org/dictionary/english/provide

[cxi] https://dictionary.cambridge.org/dictionary/english/predict

[cxii] https://dictionary.cambridge.org/dictionary/english/present

[cxiii] https://dictionary.cambridge.org/dictionary/english/recognize?q=recognise

[cxiv] https://dictionary.cambridge.org/dictionary/english/research

[cxv] https://dictionary.cambridge.org/dictionary/english/report

[cxvi] https://dictionary.cambridge.org/dictionary/english/review

[cxvii] https://dictionary.cambridge.org/dictionary/english/secure

[cxviii] https://dictionary.cambridge.org/dictionary/english/select

[cxix] https://dictionary.cambridge.org/dictionary/english/solve

[cxx] (ISO 9000:2015(en), Quality management systems — Fundamentals and vocabulary)

[cxxi] https://dictionary.cambridge.org/dictionary/english/use

[cxxii] https://dictionary.cambridge.org/dictionary/english/verify

[cxxiii] https://dictionary.cambridge.org/dictionary/english/work

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union