REWIRE
CYBERSECURITY SKILLS ALLIANCE

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

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R.4.6.2 Cybersecurity Skills Qualification Standards

Cyber Incident Responder

Title	R.4.6.2 Cybersecurity Skills Qualification Standards – Cyber Incident Responder
Document description	This document is the Cybersecurity Skills Qualification Standard (i.e., Certification scheme) for the role profile of the Cyber Incident Responder.
Nature	Public
Task	T4.6 Design of Certification Schemes for selected Cybersecurity Occupational Profiles
Status	Final
WP	WP4
Lead Partner	APIROPLUS SOLUTIONS
Partners Involved	CCC, LRQA
Date	31/07/2023

Disclaimer:

CONTENTS

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

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. EXECUTIVE SUMMARY

"Certification for persons is one means of providing assurance that the certified person meets the requirements of the certification scheme. Confidence in the respective certification schemes for persons is achieved by means of a globally accepted process of assessment and periodic re-assessments of the competence(s) of certified persons."[1]
To achieve the above mentioned goal, and have a truly valid, comparable and value adding certification scheme, this document has been created. This document is the Cybersecurity Skills Qualification Standard (i.e., Certification scheme) for the role profile of the Cyber Incident Responder.
The contents of this document are well aligned with ISO/IEC 17024:2012, Conformity assessment — General requirements for bodies operating certification of persons and to the CONCORDIA Cybersecurity Skills Certification Framework[2].
The document provides information on what the REWIRE Cyber Incident Responder certification scheme covers in terms of tasks, skills and knowledge. It outlines the different roles involved in the certification process, and comprehensively describes the examination mechanism and the system of rules, procedure and management for carrying out certification. Finally, the document presents how the basic principles of the certification scheme are fulfilled.

[1] https://www.iso.org/standard/52993.html
[2] https://www.concordia-h2020.eu/wp-content/uploads/2022/12/CONCORDIA_Certification_Framework_1.0.pdf

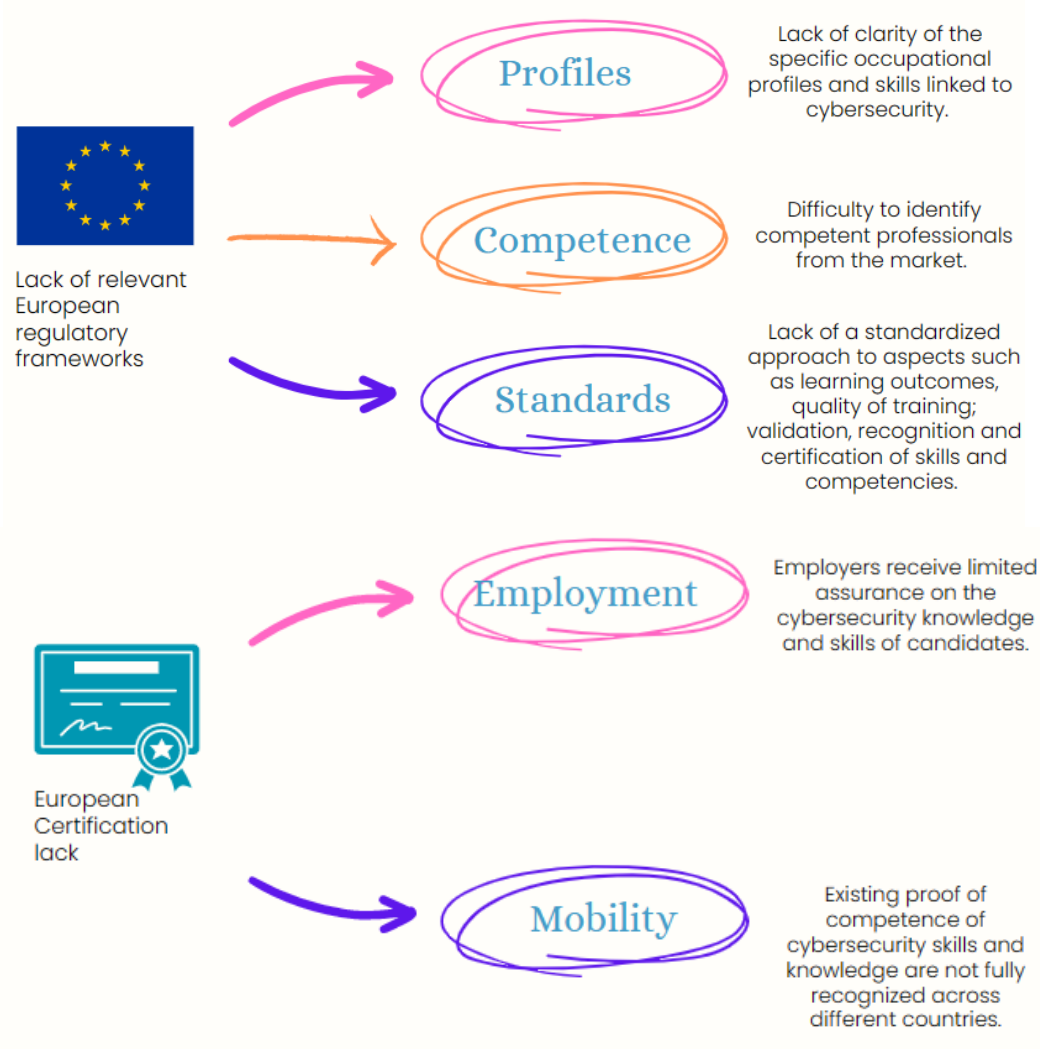
REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE Cybersecurity Skills Alliance
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

2. INTRODUCTION

2.1. Purpose

The cybersecurity skills gap has been evidenced now for many years and in various qualitative and quantitative studies such as surveys. Recent surveys and publications (e.g. ISACA[3], (ISC)[24], Fortinet[5], World Economic Forum[6] and others), indicate that although actions are being implemented to address the cybersecurity skills gap, the gap still persists and presents a barrier to cybersecurity resilience.

In the REWIRE deliverable R.2.1.1. PESTLE analysis results[7], the REWIRE team, through the implementation of a relevant PESTLE analysis, identified the following factors influencing cybersecurity education:



[3] https://www.isaca.org/go/state-of-cybersecurity-2022
[4] https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx
[5] https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf
[6] https://www.weforum.org/agenda/2020/01/why-closing-the-cybersecurity-skills-gap-starts-from-the-top/
[7] https://rewireproject.eu/wp-content/uploads/2022/04/R2.1.1-PESTLE-analysis-results_FINAL-v1.1_compressed.pdf

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

Figure 1 PESTLE analysis related factors

Taking into consideration the above-mentioned factors, the REWIRE project has proposed a strategy (Deliverable R2.3.1. Cybersecurity Skills Strategy[8]) and concrete actions, with the final aim to tackle the cybersecurity skills gap. Specifically, within the activities to improve cybersecurity skills development in a better structured and more simplified manner, the following have been identified:

Figure 2 Extract from R2.3.1. Cybersecurity Skills Strategy

A skills certification scheme contains the technical requirements and methods through which a specific skills certification activity is implemented.

2.2. About ISO/IEC 17024:2012

ISO/IEC 17024:2012[9] is an international standard developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This International Standard has been developed with the objective of achieving and promoting a globally accepted benchmark for organizations operating certification of persons.

Certification for persons is one means of providing assurance that the certified person meets the requirements of the certification scheme. Confidence in the respective certification schemes for persons is achieved by means of a globally accepted process of assessment and periodic re-assessments of the competence of certified persons.

ISO/IEC 17024:2012 can serve as the basis for the recognition of the certification bodies for persons and the certification schemes under which persons are certified, in order to facilitate their acceptance at the national and international levels. Only the harmonization of the system for developing and maintaining certification schemes for persons can establish the environment for mutual recognition and the global exchange of personnel.

[8] https://rewireproject.eu/wp-content/uploads/2022/05/R2.3.1-Cybersecurity-Skills-Strategy_FINAL-v1-compressed.pdf
[9] https://www.iso.org/standard/52993.html

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

ISO/IEC 17024:2012 specifies requirements which ensure that certification bodies for persons operating certification schemes for persons operate in a consistent, comparable and reliable manner.

The requirements in ISO/IEC 17024:2012 are considered to be general requirements for bodies providing certification of persons. Certification of persons can only occur when there is a certification scheme. The certification scheme is designed to supplement the requirements included in ISO/IEC 17024:2012 and include those requirements that the labour market needs or desires, or that are required by governments.

2.3. The CONCORDIA Cybersecurity Skills Certification Framework

The CONCORDIA Cybersecurity Skills Certification Framework[10] provides information on the minimum requirements that a certifying organization should comply with when implementing certification schemes for cybersecurity skills.

These requirements can be seen as an expansion and specialization of a selection of the ones included in ISO/IEC 17024:2012 Conformity Assessment — General Requirements For Bodies Operating Certification Of Persons, especially in the area of certification principles.

As mentioned above, the requirements in ISO/IEC 17024:2012 are generic and should be further customized to meet the specific needs of the interested parties through the design and implementation of a suitable certification scheme.

The CONCORDIA Cybersecurity Skills Certification Framework acts as a high level customization of the principles of ISO/IEC 17024:2012 within the area of cybersecurity skills.

Specifically, the CONCORDIA Cybersecurity Skills Certification Framework includes a number of requirements and information on the certification principles of:

- Impartiality – 8 Requirements
- Responsiveness – 5 Requirements
- Confidentiality – 8 Requirements
- Responsibility – 5 Requirements
- Competence – 18 Requirements

The REWIRE project has decided to adopt the principles and guidelines of the CONCORDIA Cybersecurity Skills Certification Framework, in the implementation of the relevant cybersecurity skills certification schemes.

[10] https://www.concordia-h2020.eu/wp-content/uploads/2022/12/CONCORDIA_Certification_Framework_1.0.pdf

2.4. The Cyber Incident Responder certification scheme

This document builds on the requirements of ISO/IEC 17024:2012 and the CONCORDIA Cybersecurity Skills Certification Framework and presents the technical requirements and processes to be implemented in order to support the certification of knowledge and skills of individuals for the role of the Cyber Incident Responder.

This Cyber Incident Responder certification scheme has been developed by the certification related partners of the REWIRE project and as such these partners share the ownership of this certification scheme.
These partners are also identified in the beginning of the document but are also provided hereunder for clarity purposes.

Cyprus Certification Company | LRQA Group Limited | APIROPLUS Solutions Ltd.

The responsibilities of the co-owners of the certification scheme are precisely described within the various sections of this document.

This document provides a comprehensive description of the tasks and competencies of the Cyber Incident Responder role, the scheme's technical committee, the examination mechanism, the process leading to certification, the principles and relevant processes to support the certification mechanism.

3. CYBER INCIDENT RESPONDER

The REWIRE project has analyzed the European Cybersecurity Skills Framework[11] (ECSF) profile for the Cyber Incident Responder as part of the activities for WP4 (specifically, for R4.2.1 REWIRE Curricula and Training Framework and R4.2.2 Training courses material). This analysis resulted in the formulation of the tasks, skills, knowledge and pre-requisites for the role. This section includes information about the mission, the tasks, the skills and knowledge for the occupational profile of the Cyber Incident Responder.

3.1. Cyber Incident Responder Mission

A Cyber Incident Responder plays a critical role in safeguarding organizations from cyber threats and effectively responding to cybersecurity incidents. With the increasing frequency and sophistication of cyber-attacks, organizations need skilled professionals who can identify,

[11] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

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

contain, mitigate, and recover from incidents to minimize the impact on their systems and data.

3.1. Cyber Incident Responder professional level

In general, the role of the Cyber Incident Responder resides at e-CF level 3 and EQF level 6. This would mean:

e-3		
e-cf level descriptor	**Influence**	Autonomy
Respected 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.	Consults	Works independently to resolve interactive problems and addresses complex issues. Has a positive effect on team performance.
Complexity	Structured - unpredictable	
Behaviour	Planning, making decisions, supervising, building teams, forming people, reviewing performances, finding creative solutions by application of specific technical or business knowledge/skills.	

Table 1. e-cf levels

Level		
Knowledge	**Skills**	**Responsibility and authority**
Advanced knowledge of a field of work or study, involving a critical understanding of theories and principles	Advanced skills, demonstrating mastery and innovation, required to solve complex and unpredictable problems in a	Manage complex technical or professional activities or projects, taking responsibility for decision-making in unpredictable work or study contexts;

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

	specialised field of work or study	take responsibility for managing professional development of individuals and groups

Table 2. EQF levels

3.2. Cyber Incident Responder Main Tasks

The main tasks of a cyber incident responder involve effectively responding to and managing cybersecurity incidents within an organization.
The main tasks that have been identified by ENISA and been updated and enriched by REWIRE project are the following:

Tasks	e-CF level
Analyze, collect and evaluate evidence of possible security events and incidents.	Level 3
Coordinate and advise enterprise-wide cyber defense technicians on resolution of cyber defense incidents.	Level 4
Coordinate incident response activities.	Level 4
Design, document and communicate cyber defense techniques, guidance, and reports on incident findings as needed.	Level 4
Design, document and implement cyber incident management policies, procedures and plans.	Level 4
Document and communicate as needed after action reviews, lead the lessons learned sessions etc.	Level 4
Monitor, analyze and evaluate intrusion artifacts and design and implement mitigation actions (of potential cyber defense incidents) within the enterprise.	Level 4
Monitor, analyze and evaluate network alerts from various sources within the enterprise.	Level 3, Level 4
Monitor, analyze and report on cyber defense trends.	Level 4

3.3. Cyber Incident Responder Skills

3.3.1. REWIRE project Skills Groups

REWIRE project Skills Groups	
Collaborate and Communicate	Operating Systems
Digital Forensics	Risk Management
Incident Management	Threat Analysis
Information Systems and Network Security	Workforce Management

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

Table 3. REWIRE project Skills Groups

3.3.2. Skills Based on ESCO Mapping

Skills based on ESCO mapping	
Communicate, present and report to relevant stakeholders	Recognize and categorize types of vulnerabilities and associated attacks
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)
Manage and analyse log files	Secure network communications
Recognize and categorize types of vulnerabilities and associated attacks	Use security event correlation tools
Perform damage and risk assessments (for the specific incidents and the related scenarios) identifying, capturing, containing, and reporting malware	Work on operating systems, servers, clouds and relevant infrastructures
Practice all technical, functional and operational aspects of cybersecurity incident handling and response	Perform damage and risk assessments (for the specific incidents and the related scenarios) identifying, capturing, containing, and reporting malware
Work under pressure	Collect, analyse and correlate cyber threat information originating from multiple sources

Table 4. Skills based on ESCO mapping

3.4. Cyber Incident Responder Knowledge

3.4.1. REWIRE project Knowledge Groups

REWIRE project Knowledge Groups	
Data Security	Network Management
Incident Management	Operating Systems
Information Systems and Network Security	Risk Management
Law, Policy, and Ethics	Threat Analysis

Table 5. REWIRE project Knowledge Groups

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

3.4.2. Knowledge based on ESCO

Knowledge based on ESCO mapping	
Knowledge of cloud service models and how those models can limit incident response	Knowledge of offensive and defensive security practices
Computer Security Incident Response Teams (CSIRTs) operation	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)
Incident handling standards, methodologies and frameworks	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions
Incident handling tools	Knowledge of malware analysis concepts and methodologies
Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)	Knowledge of system administration, network, and operating system hardening techniques
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks)	Cybersecurity related laws, regulations and legislations
Secure Operation Centres (SOCs) operation	Cybersecurity-related certifications
Computer networks security	Knowledge of OSI model, underlying network protocols (e.g., TCP/IP), Dynamic Host Configuration, Domain Name System (DNS), and directory services
Computer systems vulnerabilities	Knowledge of network services and protocols interactions that provide network communications
Incident handling recommendations and best practices	Cybersecurity attack procedures
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth)	Knowledge of business continuity and disaster recovery continuity of operations plans
Operating systems security	Cyber threats

Table 6. Knowledge based on ESCO mapping

4. HUMAN RESOURCES

4.1. Scheme's Technical Committee

A Certification scheme's Technical Committee, is a group of people, formed before the activation of the certification scheme and remain active as long as the certification scheme is active.
The Certification scheme's Technical Committee is essential body responsible for the adequate implementation and operation of the certification scheme and has the following responsibilities and authorities:

- The Certification scheme's Technical Committee defines the main principles and content for the certification scheme to fulfil the technical requirements for each specific Certification Scheme and develops the scheme, taking into account the interests of relevant interested parties.
- The Certification scheme's Technical Committee takes into consideration the various developments and makes proposals and suggestions for changes and improvements to the certification scheme.
- The Certification scheme's Technical Committee keeps necessary records / documented information to support accountability and traceability of changes to the certification scheme.
- The Certification scheme's Technical Committee decides on the dates and methods that the examinations of the certification scheme are carried out.
- The Certification scheme's Technical Committee evaluates and analyzes the results from the "beta" testing of the examination for the certification scheme and decide if anything within the design and operation of the certification scheme needs to be revised or proactively improved.
- The Certification scheme's Technical Committee, before the start of an examination period makes sure that all necessary supporting materials are in place exists and implemented within the systems as required.
- The Certification scheme's Technical Committee coordinates the announcement of the examination period(s), providing the necessary information to all audiences and effectively responding to request for information to relevant interested stakeholders.
- The Certification scheme's Technical Committee shall authorize the activation / opening of the application process and shall review the received applications against the pre-requisites identified as part of the certification scheme.
- The Certification scheme's Technical Committee shall implement automatic responses to be sent through the system for every step of the application, examination and certification process.
- The Certification scheme's Technical Committee is responsible for receiving and responding to complaints or objections from the interested parties in a timely manner. The Certification scheme's Technical Committee shall involve in the response other REWIRE partners or interested parties if deemed necessary.

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

- The Certification scheme's Technical Committee shall evaluate the examination mechanism, the conduct of the examinations and assessment procedure, shall review the performance and results of the examination for quality assurance purposes as well as shall propose and implement necessary changes
- The Certification scheme's Technical Committee shall make sure that the examination mechanism is valid, objective, reliable and suitable for use in future examinations.
- The Certification scheme's Technical Committee is responsible for the decision-making process of certification.

To achieve the above, the Certification scheme's Technical Committee, shall convene as appropriate and at least once a year to ensure adequate operation of the certification scheme. These meetings can take place either in person or remotely. The Certification scheme's Technical Committee shall keep minutes of the decisions taken during each meeting. The Certification scheme's Technical Committee may invite other interested parties to participate in these meetings if deemed necessary.

The Certification scheme's Technical Committee shall be comprised of 3 (three) people, each one representing the "certification related" partners of the REWIRE project. All members of the Certification scheme's Technical Committee, shall bound by non-disclosure agreements for the entire duration of their engagement within the committee and for a period of 10 years after the termination of the engagement.

4.2. Personnel related to the assessment materials

The Certification scheme's Technical Committee is sustained by the partners of the REWIRE project in the creation of the databank of examination items to support the theoretical and practical part of the examination mechanism.
The REWIRE project has created a specific guideline (Guidelines: Theoretical assessment Questions), which provides guidance to all involved parties:

- on the types of questions that can be technically implemented in the theoretical examination platform,
- on the difficulty levels of questions and
- on the applicability of the different types of questions per level of skills or knowledge (taking into consideration REWIRE deliverable: R4.6.5 Cybersecurity Skills Assessment Recommendation).

For the practical examination scenarios, directions have been provided in collaboration with the team responsible for the creation of the Cyberange platform.
The creation of the examination items (theoretical and practical) has been assigned to partners taking into consideration their competence on the role profile the certification scheme is covering, to make sure that they are suitable and will ensure a high level of quality of the examination and the produced certification.

The Certification scheme's Technical Committee collects, reviews and uploads the examination material in the relevant platforms. If during the various stages of the certification process, changes need to be undertaken on the examination items, the Certification scheme's

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

Technical Committee shall make the relevant communications and assign the implementation of the changes to the appropriate competent parties.

Individuals participating in the development, change, assessment, review or evaluation of examination items are not allowed to undertake the exams (participation in the examination) and are bound by non-disclosure agreements for the entire duration of their engagement as members of the committee and for a period of 10 years after the termination of the engagement.

4.3. Examiners

Examiners are individuals responsible for assessing learner's achievements and for the grading of an exam. Based on the design of this certification scheme, examiners are only responsible for the practical exam administered through the REWIRE project cyberange.
The examiners shall have the following minimum competency:

- Certified Educational Proficiency Generally (depending on country requirements)
- Minimum 100 hours teaching experience in the cybersecurity domain
- Minimum 5 years of professional experience in the cybersecurity domain
- Degree at a university level on Information Technology, Computing, Computer Science, Computer Engineering, Information Technology and Information Systems, Computer Networking and other similar fields of study.

Following the completion of the practical exam period, the examiners shall be assigned examination attempts and will grade them based on the design of the examination scenario.
If an examiner has a potential conflict of interest in the examination of a candidate, the Certification scheme's Technical Committee shall take the necessary measures to ensure that the confidentiality and impartiality of the examination are not compromised. These measures shall be duly recorded.
All examiners shall be bound by non-disclosure agreements for the entire duration of their engagement and for a period of 10 years after the termination of the engagement.

4.4. Invigilators

As defined within ISO 29996:2021 (Education and learning services — Vocabulary)[12], Invigilator is the authorised person who administers or supervises an assessment, ensuring fair and proper conduct of examinations.
Invigilators shall involved in the certification mechanism process to ensure that the confidentiality, integrity and impartiality of the examination is not compromised. The invigilators are not required to have specific qualifications. The invigilator may be administrative staff member of any partner of the REWIRE project. During the examination, the invigilators will verify the identity of the candidates based on relevant documents, supervise the applicants to ensure compliance with the examination procedure, closely work with the Head of examination to resolve any issues that may arise during the examination, prevents fraud involving the behaviors and actions of candidates during the examinations and complete the necessary paperwork (if applicable) etc.

[12] https://www.iso.org/standard/54664.html

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

If an invigilator has a potential conflict of interest in the examination of a candidate, the Certification scheme's Technical Committee shall undertake the necessary measures to ensure that the confidentiality and impartiality of the examination are not compromised. These measures shall be duly recorded.
All invigilators shall be bound by non-disclosure agreements for the entire duration of their engagement and for a period of 10 years after the termination of the engagement.

4.5. Other personnel supporting the certification process

Some of the supporting activities in relation to the operation of the certification mechanisms may be assigned to outsourced partners (e.g. the support of the online platform). In such cases, the partner responsible shall have a formal agreement with a clear scope and definition of responsibilities for the third parties. To the extend that such parties may have access to the examination content, the agreement shall include also a non-disclosure clause bounding the organization to confidentiality for the entire duration of their engagement and for a period of 10 years after the termination of the engagement.

5. EXAMINATION MECHANISM

5.1. General

Examination mechanisms are designed to assess candidates' qualifications based on, and consistent with, the profession, by any reliable and objective mean as written, oral and/or practical exams, observation etc. The examination requirements must ensure the comparability of results of each single examination, both in content and difficulty, including the validity of fail/ pass decisions.
The examination mechanism includes a method which can assess and verify that the candidate possesses the knowledge and skills that have been described by certification scheme requirements, either acquired by work experience, formal or non-formal learning outcomes or other means.
The examination mechanism for this certification scheme is split into two parts: theoretical and practical. In the sections below, information is provided for each one of these two parts. Since certification is not a spontaneous process, from the candidate point of view, the process starts with the application.
For the first implementations of the certification scheme, the language of all the related material shall be English. The project partners will re-consider the linguistic dimension after initial operation of the certification scheme to see if parts or all of the information related to the certification need to be translated also into other languages.

5.2. The application

To facilitate the easy and consolidated experience of the examination process, the REWIRE project has decided to utilize a customized on-line platform owner by the REWIRE project partner CCC.

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

This platform is a specially customized Learning Management System (hereafter referred as LMS).
To begin the application process, the candidate needs to first create an account in the LMS. The information regarding where and how the account can be created, shall be provided to the applicant with the rest of the information when the activation of the certification scheme and the examination period is published.
By entering the requested information into the system, the applicant will automatically receive an email to activate their account (User activation).
With the effective activation of the account, the applicant will be able to register for the desired examination by completing the relevant application form on the platform (Course application) under the 'Certification of persons' section of the platform.
The applicant must provide all personal information during the application process and, by accepting the relevant fields, affirms compliance with this regulation and all pertinent procedures.
In addition, the applicant uploads electronic proof of identity and academic credentials, or qualifications as required by the certification scheme (see below section 5.3. Prerequisites for applicants).
The application form includes the following information and data for each applicant:

- Name, surname, Father's name (optional), date of birth (optional), address, Telephone Number, Email, tax identification number (optional), special requests and contact details of the candidate (optional) and
- Evidence of pre-requisites as required by the certification scheme

The applicant receives an automated message confirming that their application has been received and that they will be notified as to whether or not it has been accepted.
If the application is approved, an email is automatically sent to the candidate with the application's status.
Any application for Certification that does not satisfy all prerequisites will be denied. In such event the applicant is notified prior to the examinations that their application has been rejected.
As mentioned above, the Certification Schemes Technical Committee undertakes the evaluation of the existence of the prerequisites based on the specified requirements of the certification scheme.
The system has the ability to assign specific number of applications to different members of the Certification Schemes Technical Committee. In the end of this evaluation process, the Certification Schemes Technical Committee convenes to reach the final decisions.
The applicant has the option of submitting new documents through a new application before the exams are held and up until the deadline for submitting applications in order to be reconsidered for the examination.
After the evaluation of completeness and approval of the application by the technical committee, each candidate can find personal information, the unique candidate number, and the exam in which they desire to participate in their personal account.

5.3. Prerequisites for applicants

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

The professionals should already have a level of IT / IS knowledge and skills at e-CF level 1 - 2 (EQF levels 3-5). Such knowledge could be substantiated by the following:

- Degree at a university level on Information Technology, Computing, Computer Science, Computer Engineering, Information Technology and Information Systems, Computer Networking and other similar.
- Vocational Education Degree on Information Technology, Computing, Computer Science, Computer Engineering, Information Technology and Information Systems, Computer Networking and other similar and experience of at least 2 years in IT or IS.
- Fulltime practical experience of at least 4 years in IT or IS.
- Professional Certification in a IS/IT subject related to cybersecurity incident response (systems administration, operational procedures, network management, monitoring tools management etc) and fulltime practical experience of at least 2 years in IT or IS.

To ensure the integrity of the process and that the certificates are awarded to specific natural persons, it is mandated that the person also submits a valid personal identification document during the prerequisites phase. This document will be also used during the theoretical and practical exams, as a proof of identity.

5.4. Theoretical examination

For the theoretical examination of skills and knowledge the following apply:

- The theoretical examination is conducted through a dedicated platform owned by the CCC partner of the REWIRE project.
- To ensure the integrity of the examination, the examination session is monitored through an invigilator. The invigilator, using the ZOOM tool, will guide the applicant on the steps to take, in order to have a view of the candidate's screen, a view (video) and sound from the candidate. These measures have been deemed mandatory in order to ensure the high value, quality and integrity of the examination mechanism and certificate.
- Information, instructions for use and encouragement for testing shall be sent to candidates prior to their examination slot.
- Each candidate may only have one attempt. For this attempt, 1 hour and 10 minutes shall be allocated.
- The theoretical examination consists of a quiz with forty five (45) questions, of two levels of difficulty (Basic and Advanced), selected randomly from the Examination Questions Bank.
- The Questions Bank includes approximately 300 different questions for evaluating the knowledge and skills described in Section 3. above. To ensure consistency of the questions, a special guideline has been provided to all examination items authors.
- For each examination item, there is a direct mapping on the Task of the role it relates to, the grades awarded, the level of difficulty and the professional level of the skills and knowledge assessed.
- In each examination attempt, the examination items shall be selected from all different tasks and all different levels equally.
- The pass mark for the quiz is 60% and is derived automatically from the platform.

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

- The score achieved by the candidate shall be displayed at the end of the examination attempt to the candidate. If there is a problem with the integrity of the exam, the invigilator has the right to stop the process at any time before the final score is provided.
- A quality review process on the databank shall be implemented at regular intervals or if complaints exist. If deficiencies are identified appropriate corrective actions shall be implemented in a timely manner.

5.5. Practical examination

The practical examination is administered through an online platform (cyber range). A transparent and user friendly instruction guide and video are provided to use the system.
The security measures implemented within the platform are at same high level and aligned with the requirements related to the theoretical exam.
The practical exam incorporates the verification of the relevant skills under one or more comprehensive scenario(s). The questions / tasks requested to be performed by the candidate do not reference or provide the solution or provide an indication of the skills being evaluated. (E.g. The question should be “identify the devices that reside in your network and create the relevant network map” and not “Run the NMAP application, in order to find other assets within your network”).
Information about the use of the platform and its abilities, at the latest when the candidate enters the practical examination environment for the first time.
The performance of the candidate, the activities implemented and the responses to the questions are recorded and timed.
With the help of the examinators, each attempt is graded based on a baseline created with each examination scenario. The system has the ability to provide hints to the candidates, but they are limited in number, do not cover the entirety of the examination scenario and for each use, a defined number of grades are deducted.
A collection of scenarios covering the same exam, fulfilling the above. Enough scenarios exist to ensure adequate coverage based on the number of iterations per period.
A quality review process on the scenarios collection shall be implemented at regular intervals or if complaints exist. If deficiencies are identified appropriate corrective actions shall be implemented in a timely manner.
As in the case of the theoretical exam, the practical exams are administered in specific time slots and have assigned invigilators who with the help of the ZOOM platform, monitor each attempt.
Each candidate may only have one attempt. For this attempt, 1 hour shall be allocated.
The practical examination consists of a series of 20 questions incorporated within one scenario selected randomly from the Examination Scenarios Bank.
The Scenarios Bank includes approximately 5 different scenarios for evaluating the skills described in Section 3. above.
For each question, there is a direct mapping on the Task of the role it relates to, the grades awarded, the level of difficulty and the professional level of the skills assessed.
The pass mark for the quiz is 80%.

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

5.6. Grading

A candidate's result in the examination is deemed positive if they successfully pass both the theoretical and practical exams. Conversely, if a candidate does not pass either of the exams, the result is considered negative. The Certification Scheme Technical Committee shall announce the final results for both successful and unsuccessful candidates within 30 calendars days from the date of the examination.

In the event that a candidate disagrees with their final result, they have the opportunity to submit an appeal within five (5) working days from the announcement of the result, following the procedures outlined by the Certification Scheme Technical Committee. The Certification Scheme Technical Committee is then required to carefully consider the appeal and provide a response to the individual within a specific timeframe (refer to paragraph 7.4, "Objections, Complaints, and Appeals") regarding the decision made regarding the filed appeals.

Participation in the examination mechanism is not limited, allowing individuals to participate as frequently as desired until they successfully pass the exam and obtain certification.

6. CERTIFICATION

6.1. Issue and award of Certificate

The Certification Scheme's Technical Committee is responsible for assessing the registration and examination procedure and validating the certification decision.
The Certification Scheme's Technical Committee must evaluate the following at a minimum:

- That the participant(s) is/are included in the participant list incorporated in the 'Results Report'.
- That the Pass/Fail results for every candidate, is recorded in the 'Results Report' for every part of the examination.
- That the examination personnel have signed the required Non-disclosure agreements and have declared no conflicts of interest exist.
- And confirms the registration for the examination, completion of candidate information, documentation of participation requirements, candidate acceptance declarations, and application approval.

If all above have been verified, the Certification Scheme's Technical Committee reaches their decisions and documents them appropriately. If the decision to issue a certificate is positive, the authorised person handling the examination platform prepares the "Certificate Terms of Use" contract, which is issued to the candidate. Since the "Certificate Terms of Use" has been returned signed, the certificate is then issued via the platform. Certificates are generated automatically, emailed to the Certified Person, and archived in their platform account.
If the decision is negative following evaluation by the Certification Scheme's Technical Committee, it is recorded in the Results Report and then the person handling the platform notifies the candidate in writing.

Each certificate issued shall include the following information:

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

- The certification scheme owners
- The name of the certification scheme
- The name and surname of the Certificate Holder
- A unique Uid of the Certificate Holder
- A reference to the version of the applicable certification scheme under which the certificate is issued
- A unique Certificate Number
- The date the certificate is issued
- The expiration date of the certificate
- The contact details within the owners of scheme, where people may address requests, complaints or any other relevant issue
- A disclaimer regarding the usage of the certificate.
- A QR code directing the interested parties to the verification website.

A sample of the certificate template is included in Annex 1.

To ensure traceability and validation capability of certificates, a register of certificates shall be maintained with at least the following information:

- Certification Scheme
- Certificate Number
- Name, Surname of the Certificate Holder
- Date of certificate acquisition
- Date of certificate expiration
- The pre-requisites

The certificates shall have a validity of 3 years. More information on how a certified person may retain the certification is included in section 6.3.
The information related to certification process shall be retained by the relevant involved partners of the REWIRE project for a period of 6 years. Indicative information of this kind may be included: the application form, the examination notifications, the results, the various decisions of the Certification Scheme Technical Committee (including the ones related to certification), information regarding performance evaluation, appeals, complaints etc.

6.2. Validation of certification information

The REWIRE project provides the public an opportunity to verify the validity of a certificate at any point of time. This process shall be anonymous for the requester.
The validation and provision of information process is designed in a way that allows for the protection of the availability, confidentiality and integrity of the information.
This activity, as a first step shall be provided through a relevant minisite within the REWIRE project website.
Each certificate (as mentioned in 6.1. above) shall have attached a QR code, which will direct any interested party to the relevant minisite within the REWIRE project website. Through this website, a query can be performed based on the number of the certificate.
The query shall provide the following results:

- Status of certificate: VALID / Invalid

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

- Name of certificate holder: xxx**** (some of the letters will be displayed only)
- Date of issue: xx/xx/xxxx

6.3. Certificate's maintenance

The certificate shall have a validity of three years. Since the cybersecurity domain is changing at a fast pace, it is crucial that certified cybersecurity professionals maintain their knowledge and skills up to date during the period of validity of the certificate.
In order for the certified professionals to maintain their certification, they need to submit (before the expiration of the certificate) to the owner of the certification scheme evidence of the implementation of suitable Continuing Professional Education activities.
A guideline shall be drafted by the scheme owners in due time regarding the type of the suitable Continual Professional Education activities, the number of suitable Continuing Professional Education (CPE) credits / points that need to be accumulated before the expiration and a method to calculate the CPEs.
This document shall include amongst others: The definition of CPEs, the activities that are eligible to provide CPEs, the correspondence between the duration of these activities and the earned CPEs, the method of reporting CPEs and the method of CPEs validation.
The owners of the certification scheme shall use the LMS platform used for administering the examination to allow the cybersecurity professionals to view, submit, change, delete, report, access, and object their CPEs per certificate.
This system also allows for the management, access and maintenance of the information needed by the certificate holder at any time. Suitable and adequate measures are enforced for the protection of the private information of the involved individuals.

6.4. Suspension and withdrawal of the Certificate

If at any point there is valid and validated proof that the certified person does not abide to the Certificate Terms of Use, or uses the certificate in a fraudulent, misleading or offensive manner, the certificate can be suspended. To suspend a certificate, the Certification Scheme Technical Committee need to convene, examine the relevant evidence and extract a majority vote for the decision to suspend the certificate.
Before reaching this point, the certified professional shall be contacted and become aware of the situation. Opportunities to remedy the situation shall be provided. In case the problems are not solved and following the decision of the Certification Scheme Technical Committee, the Certificate is suspended for a six months period. If after the six months period, the problems have still not been solved, then the Certification Scheme Technical Committee withdraws the Certificate. In case of a withdrawal, the professional has no longer the right to participate to another examination of this Scheme. The list of withdrawn certificates will be maintained by the responsible Organization.

6.5. Recertification

In the event that a certified person desires to extend their certification beyond the initial 3 year period, it is necessary for them to submit a new application to the organization

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

responsible, clearly indicating their intention to continue, no later than three months prior to the certification's expiration date.
The certified professional needs to attach evidence of the CPEs required as mentioned in 6.3. section of this document The Certification Scheme Technical Committee shall review the application and decide if the professional shall be re-certified.
After a positive relevant decision, the certificate will be reissued, retaining the same registration number, date of initial certification, date of re-certification, and a new 3-year validity period.

7. PRINCIPLES

7.1. Certificate Terms of Use (CCC)

Certified persons have to comply with the current Regulation. Certified persons must follow any revisions or additions to the Regulations if they occur in order for them to always be in compliance with the applicable obligations. Any revisions or additions to the Regulations will be communicated to certified persons in writing, and the responsible Organization, in its sole discretion, will designate a transitional period during which the certified person must abide by them.

Each Certificate is issued to the certified person (beneficiary) but remains as property of the responsible Organization until it expires or, under extraordinary circumstances, until the certified person (beneficiary) is asked to return it for the following reasons:

- at the time of application for the examination, they had submitted information which it has been found to be false or misleading,
- misleading use of the certificate by certified persons,
- a dispute or complaint regarding the certified person,
- a request by the certificated person to discontinue the use of the granted certificate

The Certificate belongs to the certified person, who must only use it for themselves and only for the certification for which they were certified. It must not be utilized in any way that would be deceptive, and the holder must present it upon demand.

Whether for any reason the certified person is unable to maintain the level of competence for which they have been certified, they must notify the responsible Organization promptly.

7.2. Confidentiality

The personal data of applicants and certified professionals remain confidential throughout the whole Certification process (from receiving the application until the issue of the certificate and its maintenance).
The owners of the certification scheme, upon request, provide information about the validity and the scope of the Certificates issued. In case the owners of the certification scheme are legally forced to reveal any confidential information, then the person interested will be informed.

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

Measures and procedures exist in all related partners of the REWIRE project regarding the response to information security incidents and personal data breaches.
Backups and any other measures deemed necessary are undertaken to ensure the availability, confidentiality and integrity of the information and the systems.

7.3. Data privacy and data retention policy

The information regarding the request of a person towards the certification scheme owner shall be collected, processed as needed, disclosed only to the roles needed and retained as needed based on a specific retention policy. A data retention policy has been designed taking into consideration amongst others the purposes of processing and the current applicable legal and regulatory requirements.
Since the information related to the certification process is personal, a data privacy policy has been created for this purpose and is provided to candidates before they enroll to the LMS system.

The policy contains the following information:

- the identity and contact details of the joined data controllers – owners of the certification scheme
- the contact details of the DPOs, where applicable
- the intended purpose of the personal data processing as well as the legal basis for processing
- the recipient or categories of recipients of the personal data, if any
- the details of any transfer, where the owners of the certification scheme intend to transfer personal data to a third country and what additional safeguards are in place.
- the period for which the personal data will be stored, or the criteria used to determine this period
- the process for the candidate to request access to and rectification or erasure of personal data or to restrict or object to processing, as well as data portability.
- the process for the candidate to withdraw consent
- the right for the candidate to lodge a complaint with the relevant supervisory authorities.
- Whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contact, as well as whether the candidate is obliged to provide the personal data and the possible consequences of the failure to do so.
- The fact that there is no use of automated decision-making, including profiling.

7.4. Objections, complaints and appeals

An interested party (candidate, examinee, certified professional, employer, third party, etc.) may wish to challenge the results of an examination at any stage of the examination process. In this case, the interested party has the option of submitting its request digitally to the Certification Scheme Technical Committee responsible for the exams. Within 30 calendar

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

days, the Certification Scheme Technical Committee must investigate the request, take corrective action if necessary, and notify the complainant in a digital manner.
The effective resolution of complaints and appeals is an important means of protecting the Certification Scheme Technical Committee responsible for the examinations and interested parties from errors, omissions or inappropriate behaviors.

7.5. Updating the assessment materials

The periodic update of assessment materials within a certification scheme is a crucial aspect of maintaining its effectiveness and relevance. Recognizing the ever-evolving nature of the cybersecurity domain, it is essential to ensure that the assessment material aligns with current industry standards, best practices, and emerging trends.
The Certification Scheme Technical Committee responsible for the certification scheme undertakes a diligent process to review and update the assessment material. This process involves engaging subject matter experts, industry professionals, and stakeholders to gather insights and relevant data regarding the knowledge, skills, and competencies required for individuals in their respective fields.
Through comprehensive analysis and validation, the assessment material is refined and updated to accurately assess the proficiency and capabilities of individuals seeking certification. This includes the review and revision of theoretical knowledge assessments, practical examinations, case studies, and any other assessment components relevant to the certification scheme.
Furthermore, the Certification Scheme Technical Committee ensures transparency and quality in the update process by adhering to established guidelines, protocols, and standards. The updated assessment material is reviewed, validated, and approved by the Certification Scheme Technical Committee to ensure its integrity and reliability.
By regularly updating the assessment material, the certification scheme not only reflects the current industry landscape but also promotes continuous professional development and maintains the credibility and value of the certification. This commitment to staying up-to-date with evolving industry demands contributes to the professional growth and proficiency of individuals holding the certification, ultimately benefiting the industry as a whole.

8. CLOSING REMARKS

The document provides information on what the REWIRE CISO certification scheme covers in terms of tasks, skills and knowledge. It outlines describes the different bodies and roles involved in the certification process, and comprehensively describes the examination mechanism and the system of rules, procedure and management for carrying out certification i. Finally, the document presents how the basic principles of the certification scheme are fulfilled.
The various requirements as described within this document, shall be implemented when the certification scheme is activated and will remain active as long as the scheme is operational. During the life-time of the certification schemes, changes will be implemented in a controlled manner, as described within the 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

9. LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/ Definition
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ISACA	Chief Information Security Officer
$(ISC)^2$	Information Systems Audit and Control Association
FORTINET	International Information Systems Security Certification Consortium
PESTLE	Global Leader of Cybersecurity Solutions and Services
CONCORDIA	Political, Economic, Social, Technological, Legal and Environmental factors
e-CF	Cyber security cOmpeteNCe fOr Research anD InnovAtion
EQF	European e-Competence Framework
ESCO	European qualifications framework
LMS	European Skills, Competences, Qualifications and Occupations
ZOOM	Learning Management System
CPE	Is a proprietary videotelephony software program developed by Zoom Video Communications

Table 7. List of abbreviations and acronyms

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

10. LIST OF FIGURES

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

11. 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

12. ANNEXES

ANNEX 1. Certificate Template