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

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R.4.6.3 Cybersecurity Skills Certification Scheme Examination material

Title	R.4.6.3 Cybersecurity Skills Certification Scheme Examination material
Document description	This document contains guidelines to support the partners in the development of the questions for the theoretical part of the assessment as well as (within the Annex) the examination database for all 4 REWIRE certification Schemes.
Nature	Public
Task	T4.6 Design of Certification Schemes for selected Cybersecurity Occupational Profiles
Status	Final
WP	WP4
Lead Partner	APIRO
Partners Involved	CCC, LRQA, URL
Date	31/07/2023

Disclaimer:

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CONTENTS

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 of certified persons."[1]

This project creates (as part of the activities of Task T4.6 Design of Certification Schemes for selected Cybersecurity Occupational Profiles) four certification schemes covering the roles of: The Chief Information Security Officer, the Cyber Threat Intelligence Specialist, the Penetration Tester and the Cyber Incident Responder.

For each one of these certification schemes, a document called Cybersecurity Skills Qualification Standard has been created and is included as part of deliverable R.4.6.2 Cybersecurity Skills Qualification Standards. The contents of these documents are aligned to ISO/IEC 17024:2012, Conformity assessment — General requirements for bodies operating certification of persons and to the CONCORDIA Cybersecurity Skills Certification Framework[2].

R.4.6.1 Cybersecurity Skills Certification Scheme Core, describes the implementation of the various common components (core) of the certification schemes (i.e., Application, policies, procedures etc).

R.4.6.2 Cybersecurity Skills Qualification Standards describe in each certification scheme (amongst others) the requirements and principles of the examination mechanisms. All 4 REWIRE certification schemes are supported by an LMS provided by partner CCC for the implementation of the theoretical part of the examination (for each certification scheme) and by the KYPO platform provided by partner MUN for the implementation of the practical part of the examination (for each certification scheme).

The document contains

- the guidelines that were provided to the partners to support the creation of the questions for the theoretical examination of each certification scheme and
- in Annex A, not available in the public version of this deliverable due to the confidential nature of the content, the theoretical and practical exam items for each certification scheme.

[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

2. INTRODUCTION

Certification of Professional's Qualifications, also known as Person's Certification, is a globally accepted process for assessment and periodic re-assessment of the competencies of certified persons.

As part of the activities of Work Package 4, and as reported within R4.2.1 REWIRE Curricula and Training Framework, four (out of the 12) of the cybersecurity profiles of the European Cybersecurity Skills Framework[3] (ECSF) were selected for the development of the relevant courses and certification schemes.

A certification scheme for skills includes the information on the scope, the job description, the required competence, the prerequisites of the candidates, the criteria for initial certification and recertification, the assessment methods for initial certification and recertification, the surveillance methods and criteria, the criteria for suspending and withdrawing certification, the storing and validating certificate information and the formulation of objections, complaints, appeals. These contents and processes are prescribed by international best practices as depicted in ISO/IEC 17024:2012 Conformity Assessment — General Requirements For Bodies Operating Certification Of Persons.

The REWIRE team has decided to adopt the CONCORDIA Cybersecurity Skills Certification Framework and as such the envisioned assessments will take place in two parts. The first part will be theoretical (covering mostly knowledge), and the second part will be practical (covering knowledge and skills) through exercises within the cyberange environment.

To support the certification schemes, the examination items (for the implementation of the assessment processes) need to be created.

This document provides details and guidance to the project team for the development of this material for the theoretical examination.

For the practical examination, due to the nature of the exam items, meetings were conducted with the support of the MUN (KYPO) team and directions were provided directly from the KYPO team to the practical exam developers, taking into considerations the principles, operation and constraints of the KYPO platform.

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

3. REQUIREMENTS FOR THE THEORETICAL ASSESSMENT

The REWIRE project team has selected the following profiles and is in the process of developing the respective cybersecurity skills certification schemes:

- Chief Information Security Officer
- Cybersecurity Incident Responder
- Penetration Tester
- Cyber Threat Intelligence Specialist

For each one of these profiles, the envisioned professional level has been identified.
Chief Information Security Officer: The knowledge and skills of the professionals achieving this certification should be residing mainly at e-CF[4] level 4 and 5 and EQF level 7 and 8. (Participants to the course should have as pre-requisites IT / IS knowledge and skills at e-CF level 2 – 3 (EQF levels 5-6) and would acquire the relevant skills and knowledge as part of the training course). The level of each of the skills and knowledge is provided also in other deliverables of the REWIRE project under WP3.
Cybersecurity Incident Responder: The knowledge and skills of the professionals achieving this certification should be residing mainly at e-CF level 3 and EQF level 6. (Participants to the course should have as pre-requisites level of IT / IS knowledge and skills at e-CF level 1 - 2 (EQF levels 3-5) and would acquire the relevant skills and knowledge as part of the training course). The level of each of the skills and knowledge is provided also in other deliverables of the REWIRE project under WP3.
Penetration Tester: The knowledge and skills of the professionals achieving this certification should be residing mainly at e-CF level 2 and EQF level 4 and 5. (Participants to the course should have as pre-requisites level of IT / IS knowledge and skills at e-CF level 1 - 2 (EQF levels 3-5) and would acquire the relevant skills and knowledge as part of the training course). The level of each of the skills and knowledge is provided also in other deliverables of the REWIRE project under WP3.
Cyber Threat Intelligence Specialist: The knowledge and skills of the professionals achieving this certification should be residing mainly at e-CF level 1 and EQF level 3. (Participants to the course should have as pre-requisites level of IT / IS knowledge and skills at e-CF level 1 (EQF levels 3) and would acquire the relevant skills and knowledge as part of the training course). The level of each of the skills and knowledge is provided also in other deliverables of the REWIRE project under WP3.

Based on the above, the following theoretical questions should be created for each one of the profiles. For convenience purposes and to facilitate the assignment of work to partners, the requirements for theoretical questions have been split into the different modules of the respective course.

[4] E-CF levels depicted in Annex B - EQF levels description at https://europa.eu/europass/en/description-eight-eqf-levels, E-cf

Profile	Module	Number of Questions	Split	
Chief Information Security Officer	LM0 - CISO Introduction	15	Basic	10
			Advanced	5
	LM1 – Risk Management	30	Basic	15
			Advanced	15
	LM2 – Information Security Strategy	30	Basic	15
			Advanced	15
	LM3 – Incident Management	30	Basic	15
			Advanced	15
	LM4 – Business Continuity	30	Basic	15
			Advanced	15
	LM5 – Enterprise architecture and Infrastructure Design	30	Basic	15
			Advanced	15
	LM6 – Audit and Information Security Assessment	30	Basic	15
			Advanced	15
Cybersecurity Incident Responder	LM0 - Introduction	15	Basic	10
			Advanced	5
	LM1 – Risk Management	30	Basic	15
			Advanced	15
	LM2 – Incident Management	30	Basic	15
			Advanced	15
	LM3 – Information Systems and Network Security	30	Basic	15
			Advanced	15
	LM4 – Digital Forensics and Threat Analysis	30	Basic	15
			Advanced	15
Penetration Tester	LM0 - Introduction	15	Basic	10
			Advanced	5
	LM1 – Threat Intelligence Analysis	30	Basic	15
			Advanced	15
	LM2 – Information Systems and Network Security	30	Basic	15
			Advanced	15
	LM3 – Software Development and Vulnerability Assessment	30	Basic	15
			Advanced	15
	LM4 – Testing and Evaluation	30	Basic	15
			Advanced	15
Cyber Threat Intelligence Specialist	LM0 - Introduction	15	Basic	10
			Advanced	5
	LM1 – Threat Intelligence Analysis	30	Basic	15
			Advanced	15
	LM2 – Threat Analysis	30	Basic	15

Profile	Module	Number of Questions	Split	
			Advanced	15
	LM3 – Incident Management	30	Basic	15
			Advanced	15
	LM4 – Testing Evaluation	30	Basic	15
			Advanced	15

Table 1. Theoretical questions should be created for each one of the profiles

The questions shall be collected by APIRO, CCC and LRQA, will be reviewed and will be imported to the Theoretical Exams platform hosted by CCC.
For the construction of the questions, partners should take note of the guidelines provided in the next sections and provide their feedback (assigned questions) using the template provided in Annex A.

4. GUIDANCE ON THE QUESTIONS

4.1 Types of questions

The questions developed as part of the theoretical assessment as described above, will include different types of questions.

True or False questions. There is only one correct answer.

Single Choice questions: There is only one correct answer out of five options.

Multiple Choice questions: This type of question supports multiple correct answers out of five options. Users must select all the correct answers for the question to be marked correct. If they choose only some correct answers, the question is marked incorrect.

Free Choice or text input questions: This type of question provides the users with an input field where they must type the correct answer. The answers may contain one or multiple words, and the correct ones can be more than one. Capitalisation of the key words does not matter.

Matrix sorting questions: This type of question should be used when you want the candidate to match two items together. Two elements must be configured: a) Criterion and b) Sort elements or options. The latter is what users will drag & drop to the correct criterion. The options should be unique, and only one-to-one associations can be supported. The answer area will be set up like a table, with the criterion on the left and an open space to drag & drop sort elements on the right.

Sorting Choice questions: Sorting choice questions ask the user to place a series of answers in the correct order. When creating the question, the order of the answers in the backend will be considered as the correct order.

4.2 Instructions on the difficulty

In R.4.5.6. Cybersecurity Skills Assessment Recommendation[5], we have tried to correlate the type of questions and the level of the examined knowledge or skill.
In short, the results of this analysis were the following:

Type of question	EQF Level (1-8)	e-CF level (1-5)
True or False questions	1	1
Single Choice questions	1 2	1 2
Multiple Choice questions	1 2 3	1 2
Free Choice or text input questions[6]	1 2 3 4 …	1 2 3 …
Matrix sorting questions	1 2 3 4 …	1 2 3 …
Sorting Choice questions	1 2 3 4 …	1 2 3 …

Table 2. Analysis of questions (level of the examined knowledge or skill)

Based on the level of the knowledge and the skill that the participant should exhibit, the suitable type of question should be selected. This would then represent the Basic level questions for the specific competence.
Advanced level questions, should either use a more difficult type of question or should be constructed in such a way as to have an increased level of difficulty for the candidate.

[5] https://rewireproject.eu/wp-content/uploads/2023/02/REWIRE_R4.5.6_Web-1.pdf

[6] Free Choice or text input questions need a specific pool of words to be deemed correct automatically and need special attention when drafting. Please use this type as little as possible and only if the words are very specific (e.g., a definition. See also in examples below).

5. EXAMPLES

In the following tables, examples of different type of questions and of different difficulty are presented for the same topic (Risk Management Terms and Definitions)

Example Question	Characteristics	
Question: Risk is means by which a potential security incident might occur. **Answers:** **1.** True **2.** False	**Type of question**	True or False questions.
	Topic of the question	Terms and definitions of Risk Management.
	EQF level	1
	e-CF level	1
	Difficulty of the question	Basic

Table 3. Example Question (True or False)

Example Question	Characteristics	
Question: Which of the following is the correct definition of risk based on ISO 9000? **Answers:** **1.** The means by which a potential security incident might occur. **2.** The likelihood of a potential incident happening. **3.** The likelihood of a potential security event happening. **4.** The effect of uncertainly on objectives. **5.** The impact to an organization in case of fire.	**Type of question**	Single Choice questions.
	Topic of the question	Terms and definitions of Risk Management.
	EQF level	2
	e-CF level	1
	Difficulty of the question	Basic

Table 4. Example Question (Single Choice)

Example Question	Characteristics	
Question: Which of the following (select 2 out of 5) are correct cybersecurity risk statements? **Answers:** **1.** Retrieval of recycled or discarded media **2.** Failure of air-conditioning or water supply system **3.** Software malfunction. **4.** Unauthorized access to company information, through the forging of rights due to poor password management. **5.** Loss of company information through the destruction of equipment, due to inadequate or careless use of physical access control to buildings and room.	**Type of question**	Multiple Choice questions.
	Topic of the question	Terms and definitions of Risk Management.
	EQF level	3
	e-CF level	1
	Difficulty of the question	Basic

Table 5. Example Question (Multiple Choice)

Example Question	Characteristics	
Question: Provide the correct definition of risk based on ISO 9000. **Answers:** effect uncertainly objectives	**Type of question**	Free Choice or text input questions.
	Topic of the question	Terms and definitions of Risk Management.
	EQF level	1
	e-CF level	1
	Difficulty of the question	Advanced

Table 6. Example Question (Free Choice or text input)

Example Question	Characteristics	
Question: Match the examples in the number column to the terms in the column next to it with the letters. **Answers:** **1.** Flood. **2.** Error in use. **3.** Single point of failure. **4.** Eavesdropping. **5.** Lack of documentation A. Threat B. Threat C. Vulnerability D. Threat E. Vulnerability	**Type of question**	Matrix sorting questions
	Topic of the question	Terms and definitions of Risk Management.
	EQF level	3
	e-CF level	1
	Difficulty of the question	Basic

Table 7. Example Question (Matrix sorting)

Example Question	Characteristics	
Question: Sort the following threat statements from Accidental to Deliberate. **Answers:** **1.** Equipment failure **2.** Error in use **3.** Forging of rights **4.** Eavesdropping **5.** Retrieval of recycled or discarded media	**Type of question**	Sorting Choice questions.
	Topic of the question	Terms and definitions of Risk Management.
	EQF level	3
	e-CF level	1
	Difficulty of the question	Advanced

Table 8. Example Question (Sorting Choice)

6. CLOSING REMARKS

The REWIRE project creates (as part of the activities of Task T4.6 Design of Certification Schemes for selected Cybersecurity Occupational Profiles) four certification schemes covering the roles of: the Chief Information Security Officer, the Cyber Threat Intelligence Specialist, the Penetration Tester and the Cyber Incident Responder.

For each one of these certification schemes, a document called Cybersecurity Skills Qualification Standard has been created and is included as part of deliverable R.4.6.2 Cybersecurity Skills Qualification Standards. The contents of these documents are aligned to ISO/IEC 17024:2012, Conformity assessment — General requirements for bodies operating certification of persons and to the CONCORDIA Cybersecurity Skills Certification Framework[7].

R.4.6.1 Cybersecurity Skills Certification Scheme Core, describes the implementation of the various common components (core) of the certification schemes (i.e., Application, policies, procedures etc).

R.4.6.2 Cybersecurity Skills Qualification Standards describe in each certification scheme (amongst others) the requirements and principles of the examination mechanisms. All 4 REWIRE certification schemes are supported by an LMS provided by partner CCC for the implementation of the theoretical part of the examination (for each certification scheme) and by the KYPO platform provided by partner MUN for the implementation of the practical part of the examination (for each certification scheme).

This document contains

- the guidelines that were provided to the partners to support the creation of the questions for the theoretical examination of each certification scheme and
- in Annex A, not available in the public version of this deliverable due to the confidential nature of the content, the theoretical and practical exam items for each certification scheme.

The information will be updated accordingly based on the pilot implementations of the certification schemes.

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

7. LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/ Definition
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
CONCORDIA	Cyber security cOmpeteNCe fOr Research anD InnovAtion
e-CF	European e-Competence Framework
EQF	European Qualifications Framework
ECSF	European Cybersecurity Skills Framework
CISO	Chief Information Security Officer

Table 9. List of abbreviations and acronyms

8. LIST OF TABLES

9. ANNEXES

Profile	☐ CISO ☐ Cyber Incident Responder ☐Threat Intelligence Specialist ☐Penetration Tester

Q1.

Difficulty of the question: ☐ Basic or ☐ Advanced

Type of question:

☐ True or False questions
☐ Single Choice questions
☐ Multiple Choice questions

☐ Free Choice or text input questions*
☐ Matrix sorting questions
☐ Sorting Choice questions

[Description of Question 1]

Answers:

[Possible answers and the correct answer as indicated in the samples provided in **Error! Reference source not found.** depending on the type of the question]

…