

3RD EUROPEAN CYBERSECURITY SKILLS CONFERENCE

Building an EU Professional Attestation Scheme

Chatzopoulou Argyro
APIROPLUS Solutions

Co-organized by Hungary and ENISA



**EUROPEAN
CYBERSECURITY
SKILLS CONFERENCE**

Budapest

Assessment of skills



They believe that they have the specific knowledge, skills and e-competencies necessary to be able to fulfill effectively the tasks of a specific role.

What is an attestation of skills



They identify an assessment scheme, containing specific

- competencies (i.e., ability to apply knowledge and skills to achieve intended results) and
- other requirements related to the specific occupational profile.

What is an attestation of skills



They undergo, an assessment that evaluates the fulfilment of the requirements of the assessment scheme.

A part of the assessment is an examination which measures a candidate's competence by one or more means, such as written, oral, practical and observational, as defined in the certification scheme.

What is an attestation of skills



They receive an attestation, indicating that they have fulfilled the requirements and as such they have demonstrated that they fulfill

- competencies (i.e., ability to apply knowledge and skills to achieve intended results) and
- other requirements related to the specific occupational profile.

Attestation or 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.

Currently,...



ISO/IEC 17024:2012(en) ×

ISO/IEC 17024:2012(en) Conformity assessment — General requirements for bodies operating certification of persons

has been developed with the objective of achieving and promoting a globally accepted benchmark for organizations operating certification of persons.

This standard provides a minimum set of requirements for the certification bodies (and their activities) through which they determine that a person fulfils certification requirements, including application, assessment, decision on certification, recertification and use of certificates and logos/marks.



Currently,...

CONCORDIA Cybersecurity Skills Certification Framework uses as a baseline the principles presented by ISO 17024 and provides additional requirements for the specific area of cybersecurity skills.

The document includes a number of requirements and information on the certification principles of

- Impartiality** (8 requirements),
- Responsiveness** (5 requirements),
- Confidentiality** (8 requirements),
- Responsibility** (5 requirements) and
- Competence** (18 requirements).



Horizon 2020 Program (2014-2020)
Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018



Cyber security cOmpeteNCe fOR Research and InnovAtion¹

Work package 5: Exploitation, dissemination, certification and standardization
Deliverable D5.#: CONCORDIA Cybersecurity Skills Certification Framework

Abstract: This document contains CONCORDIA's recommendation for a Cybersecurity Skills Certification Framework. The document is aligned to and provides further specification on the requirements of ISO/IEC 17024:2012 CONFORMITY ASSESSMENT — GENERAL REQUIREMENTS FOR BODIES OPERATING CERTIFICATION OF PERSONS

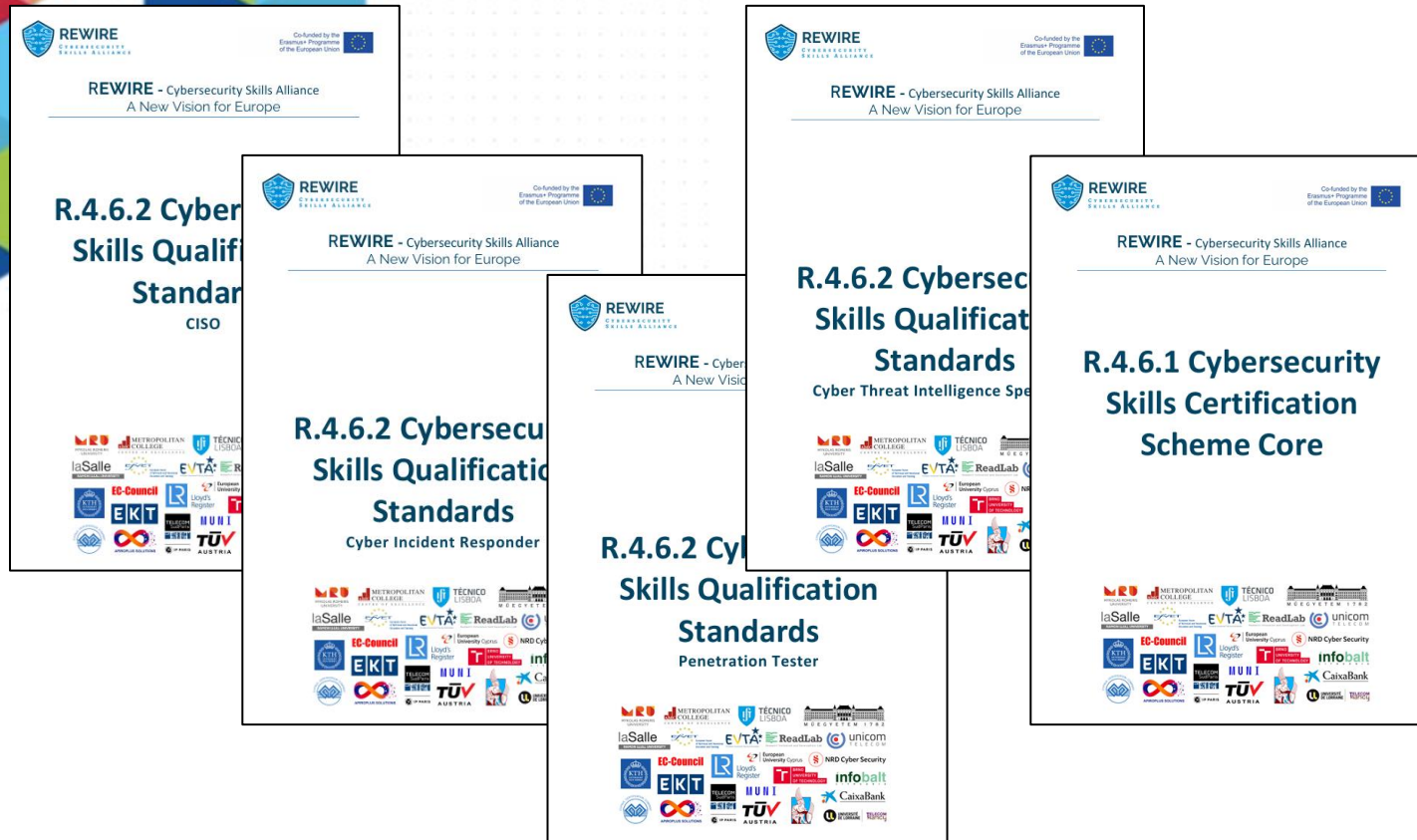
Contractual Date of Delivery	N/A
Actual Date of Delivery	31/03/2022
Deliverable Dissemination Level	Public
Editors	Chatzopoulou Argyro (TUV)
Contributors	Anisetti Marco (UMIL) Badonnel Remi (UL) Bena Nicola (UMIL) Carminati Barbara (UI) Cholez Thibault (UL) Cutas Felicia (EIT DIGITAL) Ferrari Elena (UI) Fournaris Apostolos (ISI) Franco Muriel (UZH) Prelipcean Dumitru Bogdan (BITDEFENDER)

¹ This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.



Budapest

REWIRE Certification schemes



Built adhering to: the requirements of ISO/IEC 17024 and the CONCORDIA Cybersecurity Certification Scheme, and using the respective four ECSF profiles as basis.

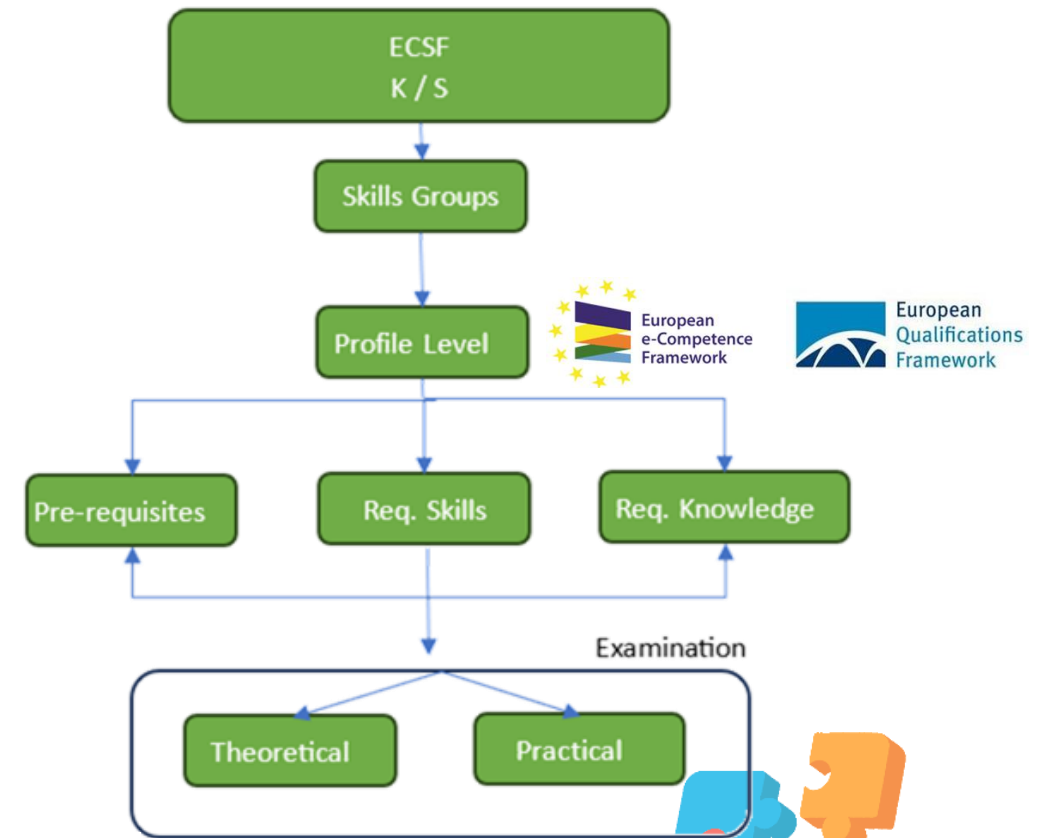


Results from piloting the schemes

Using the ECSF as a basis for certification




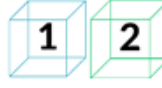

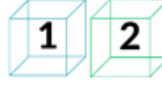

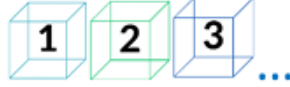

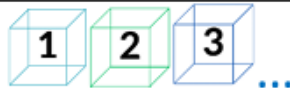

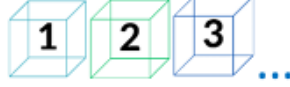
- knowledge and skills are not correlated to tasks
- the level of tasks, knowledge and skills is not provided
- the tasks, skills and knowledge are not presented in a standardized manner

The REWIRE approach



Results from piloting the schemes

Creating theoretical questions to fit the different levels of skills and knowledge

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

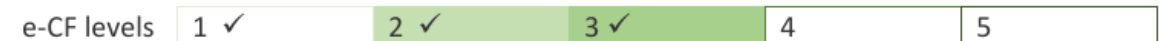
The REWIRE approach 

Results from piloting the schemes

Creating practical examinations to fit the different levels of skills, aligned to the different task



- EQF 1: Basic skills required to carry out simple tasks.
- EQF 2: Basic cognitive and practical skills required to use relevant information in order to carry out tasks and to solve routine problems using simple rules and tools.
- EQF 3: A range of cognitive and practical skills required to accomplish tasks and solve problems by selecting and applying basic methods, tools, materials and information.
- EQF 4: A range of cognitive and practical skills required to generate solutions to specific problems in a field of work or study.
- EQF 5: A comprehensive range of cognitive and practical skills required to develop creative solutions to abstract problems.
- EQF 6: Advanced skills, demonstrating mastery and innovation, required to solve complex and unpredictable problems in a specialised field of work or study.
- EQF 7: Specialised problem-solving skills required in research and/or innovation in order to develop new knowledge and procedures and to integrate knowledge from different fields.
- EQF 8: The most advanced and specialised skills and techniques, including synthesis and evaluation, required to solve critical problems in research and/or innovation and to extend and redefine existing knowledge or professional practice.



- e-CF 1: Apply knowledge and skills to solve straight forward problems;
- e-CF 2: Uses theoretical knowledge and practical skills to solve complex problems within a predictable and sometimes unpredictable context.
- e-CF 3: Providing leadership and taking responsibility for team performances and development in unpredictable environments.
- e-CF 4: Deploying specialised integration capability in complex environments; strategic development of staff working in unfamiliar and unpredictable situations.
- e-CF 5: Providing innovative solutions and for shaping the future using outstanding leading edge thinking and knowledge.

The REWIRE approach 



Thank you!

Köszönöm

3RD EUROPEAN CYBERSECURITY SKILLS CONFERENCE

Building an EU Professional Attestation Scheme

Chloé BLONDEAU
ENISA

Co-organized by Hungary and ENISA



**EUROPEAN
CYBERSECURITY
SKILLS CONFERENCE**

Budapest

ENISA Mandate



European Commission Communication of April 2023

- Propose a EU attestation for professional Cyber Skills

ENISA to:

- Develop an assessment scheme and a governance for delivering attestations
- Receive the endorsement of MS
- Launch pilots



State of Play at Member State level 1/2



- **8** member States have an **assessment programme in place** to assess cyber skills;
- **Cybersecurity Risk Managers** and **auditors** followed by **Incident Responders** are the three profiles coming back frequently in the existing or in-development certifications or training;
- The assessment of professional cyber skills is often primarily perceived as a means **to fulfill national requirements**, rather than being recognized as a valuable Human Resource tool.
- Assessment of competences remains voluntary in a large majority of Member States. **But** one third of respondents mentioned **it could become mandatory** to address specific case such as certification and the application of NIS2;

State of Play at Member State level 2/2

Existing Assessment Methods

Examination & experienced based:

- Review of curriculum based on clear requirements + examination under the control of the national authority.
- **Minimum of continuous training required and fixed validity period.**
- Publication of certified individuals (upon their agreement).
- Scope on specific missions: auditors, cybersecurity managers

Ad-hoc Examination

- Technical Interview led by the National Agency.
- Scope on a specific mission: i.e. auditors, cybersecurity managers.
- Knowledge requirements based on international standards.
- Potential Examination of the Curriculum

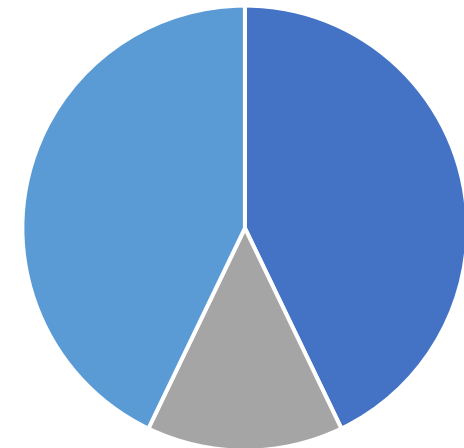
Certificate of Attendance

- Potential review of the curriculum to attend the training
- The agency provides the training or delegate it to a private organisation. In some case the syllabus is supervised by the national agency.
- Scope on a specific mission: i.e. auditors, cybersecurity managers

Labelling University programmes

- The national agency sets requirements on the content of the programme
- Fixed validity period regular review and of the programme and syllabus
- Labelling of the University programme

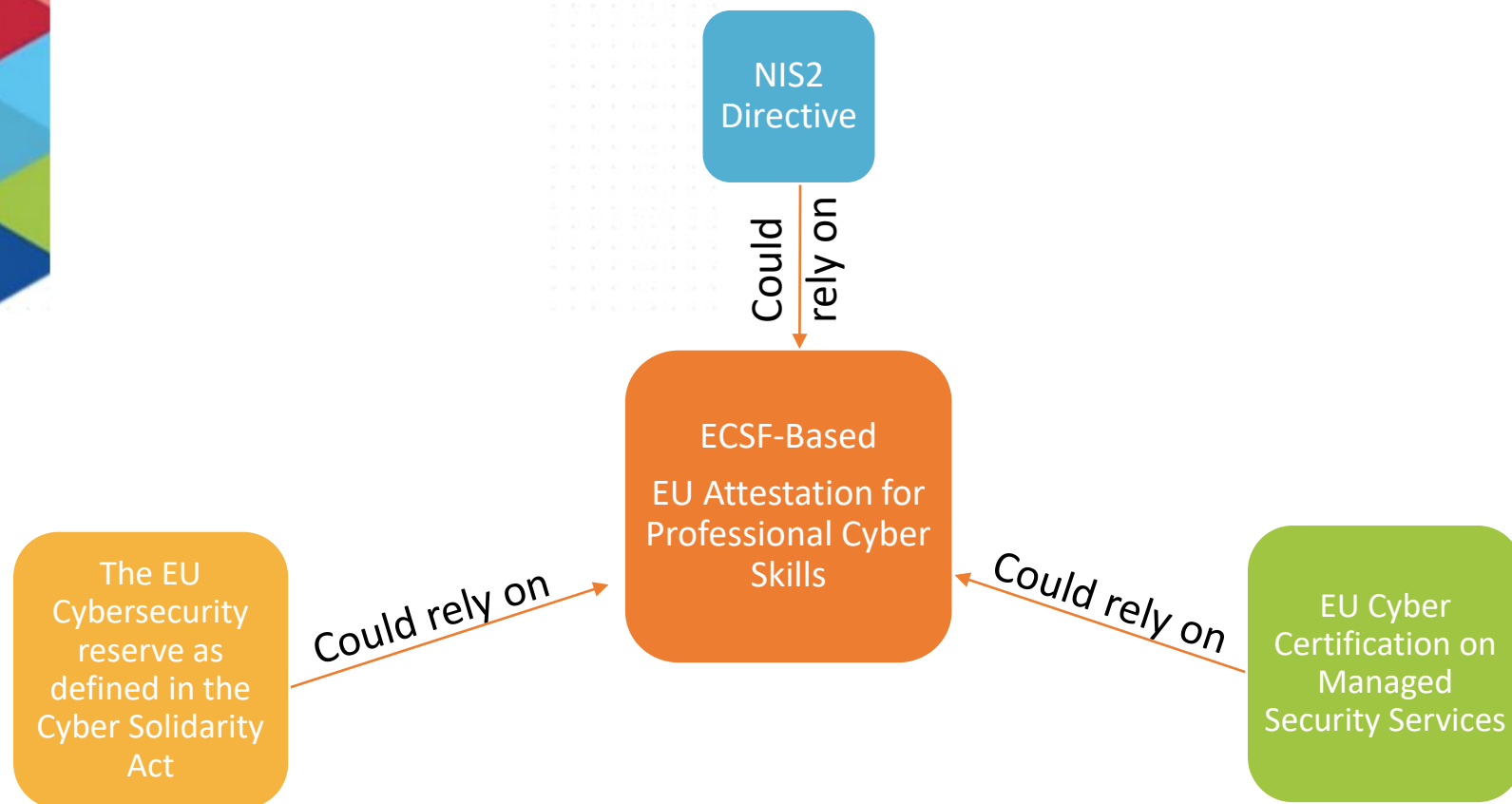
MS Trends in Cyber Skills Assessment Methods



- Training resulting into certificate of attendance
- Individual self-assessment
- Test or interview by third party



Developing a Scheme: Use Case



Select one profile to pilot:
ECSF Incident Responder

Developing a Scheme: Action Plan

Map Competencies

Define 3 levels of competences for ECSF targeted profile:

Incident Responder

Can Support regulatory needs (NIS2, CySoA, CSA)

Define Assessment Framework(s)

Deepen the understanding of the current state of play

Propose approaches based on target scenarios

Propose Scenarios

Identify 1 or 2 scenarios for an attestation of cyber Skills

Present for MS validation Scenarios to pilot



Thank you!

Köszönöm