



REWIRE - Cybersecurity Skills Alliance

A New Vision for Europe

R4.5.6. Cybersecurity Skills Assessment Recommendation



Title	R4.5.6. Cybersecurity Skills Assessment Recommendation
Document description	This document report contains recommendations describing the best practices related to examination and certification methods of the different skills and knowledge of the role profiles. These recommendations are built upon the ECSF and focus of the methods of assessment.
Nature	Public
Task	T4.6. Design of Certification Schemes for selected Cybersecurity Occupational Profiles
Status	(F: final; D: draft ; RD: revised draft)
WP	WP4 Blueprint Toolbox - Tools directly connected to education, training and certification.
Lead Partner	LRQA
Partners Involved	APIROPLUS, EKT, UL, EUC, URL
Date	31/12/2022

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	3
2. Introduction	4
2.1. Related Terms and Definitions.....	4
2.2. Relevant Standards	7
2.3. The CONCORDIA Cybersecurity Skills Certification Framework	7
2.4. Open questions	9
3. Proficiency levels	9
3.1. Topics to consider when deciding tasks.....	16
4. Assessment methods	18
4.1. Assessment of cybersecurity knowledge	18
4.2. Assessment of cybersecurity skills	20
4.2.1. Theory on practical cybersecurity skills assessment	21
4.2.2. Multiple choice questions approach	21
4.2.3. A simulation based approach	22
4.2.4. A Gamified approach	24
4.2.5. Other types of exercises	27
4.2.6. Cyber ranges as an assessment platform	27
5. Conclusions	29
6. List of Abbreviations and Acronyms	31
7. List of Figures	32
8. List of Tables.....	33

1. Executive Summary

The ECSF describes the skills, knowledge and e-competencies that each person undertaking one of the 12 roles (included in the ECSF) should have to implement the role effectively. It is essential that these skills, knowledge and e-competencies are evaluated through adequate and effective methods.

This document, presents the developments and theoretical information regarding Cybersecurity skills assessment, builds on the information extracted from the CONCORDIA project and identifies the different assessment methods for cybersecurity knowledge and skills.

The information contained within this recommendation, will be used as input in the following activities of the REWIRE project for Cybersecurity Skills Certification.

2. Introduction

As mentioned in the Executive Summary this document relates to assessment methods for Cybersecurity skills.

To be able to effectively convey the recommendations on Cybersecurity Skills assessment methods, it is important first to build a common understanding on the various terms and definitions as well as on the existing standards and frameworks.

Section 2.1. introduces the related terms and definitions based on current standards.

Section 2.2. introduces the relevant standards

Section 2.3. provides an overview of the CONCORDIA Cybersecurity Skills Framework and

Section 2.4. presents that gaps related to Cybersecurity Skills assessment that have not been filled by standards and frameworks.

2.1. Related Terms and Definitions

The European Cybersecurity Skills Framework (ECSF) is the result of the joint effort of ENISA and the ENISA Ad-hoc working group on Cybersecurity Skills Framework.

The aim of the ECSF is to create a common understanding of the relevant roles, competencies, skills and knowledge; to facilitate cybersecurity skills recognition; and to support the design of cybersecurity-related training programs. It summarizes all cybersecurity-related roles into 12 profiles, which are individually analyzed into the details of the responsibilities, skills, synergies and interdependencies it corresponds to.¹

The assessment methods presented within this document, aim to evaluate that people have the necessary knowledge, skills and e-competencies in order to implement the role effectively.

The following table contains some of the key terms related to the ECSF and the assessment of cybersecurity skills.

Term	Definition	Reference
Competence	Demonstrated ability to apply knowledge, skills and attitudes to achieve observable results. Competences form part of the Role Profiles. A demonstrated ability to apply knowledge, skills and attitudes for achieving observable results.	(CEN, 2018 ²) (CEN/TC 428, 2020 ³)
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. Knowledge is a body of information applied directly to the	(CEN, 2018) (NIST, 2018 ⁴) (CEN/TC 428, 2020)

¹ <https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework>

² CWA 16458-3:2018, European ICT professional role profiles - Part 3: Methodology documentation. Retrieved from Ecompetencies:<https://www.ecompetences.eu/ict-professional-profiles/>

³ CEN/TC 428. (2020). Methodology of the e-cf.

⁴ NIST. (2018). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Retrieved from NIST: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>

Term	Definition	Reference
	performance of a function. Represents the “set of know-what” (e.g. programming languages, design tools...) and can be described by operational descriptions.	
Role	A role derives from an organizational need to get something done. It is an organizational requirement that can be met by assigning employees to carry out all or part of the tasks required to ensure that role is carried out. One person or team may have multiple roles.	(CEN, 2018)
Role Profile	An outline or general document which demonstrates clearly the relationship between specific activities/tasks in a role and the individual skills, competences and knowledge required to undertake them.	(CEN, 2018)
Skill	The ability to use know-how and expertise to complete tasks and solve problems. 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. The ability to carry out managerial or technical tasks.	(CEN, 2018) (NIST, 2018) (CEN/TC 428, 2020)
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.	(NIST, 2018)
Tasks	A list of typical tasks performed by the profiled role.	User Manual European Cybersecurity Skills Framework (ECSF), September 2022
Work Roles	Work roles are the most detailed groupings of cybersecurity and related work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role.	(NIST, 2018)

Term	Definition	Reference
Ability	Is competence to perform an observable behavior or a behavior that results in an observable product.	(NIST, 2018)
Attitude	The “cognitive and relational capacity” (e.g. analysis capacity, synthesis capacity, flexibility, pragmatism...). If skills are the components, attitudes are the glue, which keeps them together.	(CEN/TC 428, 2020)
Assessment	<p>Assessment is normally referred to as the stage in which an individual’s learning outcomes are compared against specific reference points and/or standards.</p> <p>This can imply evaluation of written and documentary evidence but might also involve evaluation of other forms of evidence. Assessment is crucial to the overall credibility of validation of non-formal and informal learning.</p>	<p>Cedefop (2015). European guidelines for validating non-formal and informal learning. Luxembourg: Publications Office. Cedefop reference series; No 104. http://dx.doi.org/10.2801/008370</p>
Validation of learning outcomes	The confirmation by a competent body that learning outcomes (knowledge, skills and/or competences) acquired by an individual in a formal, non-formal or informal setting have been assessed against predefined criteria and are compliant with the requirements of a validation standard. Validation typically leads to certification.	<p>European guidelines for validating non-formal and informal learning Luxembourg: Office for Official Publications of the European Communities, 2009</p>
Cyberrange	<p>Cyber ranges are interactive, simulated representations of an organization’s local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing.</p> <p>A cyber range may include actual hardware and software or may be a combination of actual and</p>	NIST, Cyberranges (2018) ⁵

⁵ https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

Term	Definition	Reference
	virtual components. Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer.	

Table 1. Related Terms and Definitions

2.2. Relevant Standards

Certification for persons is a way of providing assurance that the certified person meets the requirements of a specific 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.

The principles governing these processes mentioned above are included in the ISO 17024:2012 Standard⁶.

The international Standard ISO/IEC 17024:2012 “Conformity assessment– General requirements for bodies operating certification of persons”, provides a global benchmark for quality certification. During recent years, this standard, developed by the International Organization for Standardization (ISO), which represents members from 162 countries has changed the way certifications are offered and has harmonized expectations for what constitutes quality certifications throughout the world. This standard was developed by ISO based on the need for public protection by establishing that individuals have the required competencies to perform their job⁷. Organizations worldwide have recognized the standard as a critical requirement for personnel certification bodies that offer certification in many industries including diverse and critical areas related to public health, environment, and national security.

2.3. The CONCORDIA Cybersecurity Skills Certification Framework

As part of Task T3.4 - Establishing a European Education Ecosystem for Cybersecurity, the CONCORDIA project has implemented various activities in relation to cybersecurity skills training courses. (More information can be found at <https://www.concordia-h2020.eu/concordia-service-cybersecurity-skills/>). During these activities, a gap was identified in relation to the certification of the knowledge, skills and abilities of cybersecurity professionals. Specifically, although many certification schemes exist in the are of

⁶ INTERNATIONAL STANDARD ISO/IEC 17024, Second edition, 2012-07-01, Conformity assessment — General requirements for bodies operating certification of persons, ISO (International Organization for Standardization)

⁷ [Guidelines on Conformity Assessment – ISO / IEC 17024:2012, The European Union’s 10th EDF Programme for Nigeria, United Nations Industrial Development Organization, Federal Government of Nigeria](#)

cybersecurity skills, there is no common approach and baseline leading to a fragmentation of the market and a reduction to the possible value of such certifications.

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.

It should be noted that not all of the requirements of ISO/IEC 17024:2012 are included in this document. It is envisaged that the certifying organization will follow all of the requirements of ISO/IEC 17024:2012 with the addition of the ones mentioned within this document, as specialization to the cybersecurity skills domain.

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).

For the purpose of this document, the most relevant recommendations are the following:

- 3.6.6. For each **identified knowledge and skill**, the organization shall adopt a **relationship between the e-competency proficiency level** as applicable (e.g. If a given Role Profile contains → Dimension 1: A. Plan, Dimension 2, e-competency: A.6. Application Design, Dimension 3, e-competency proficiency levels 1,2 and 3, K2 Software development methods and their rationale, there would need to be a definition whether this knowledge (K2) is needed at a level 1, 2 or 3.) This will in turn allow for the definition of the **content and level of the questions / tests that should be included in the examination for the validation of this knowledge**. The same distinction should be applied for skills also.
- 3.6.7. In every examination, all knowledge and skills identified within the certification scheme shall be assessed.
- 3.6.8. **Knowledge should be at least theoretically validated**. The certifying organization may use multiple choice, open ended or scenario-based questions.
- 3.6.9. Since skills are more about applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual, the **majority of the skills should be examined in a practical manner**.
- 3.6.10. Roles identified in **e-Competence levels 2-5 should test / verify the identified skills and knowledge (if desired) in a practical manner**. The Certifying organization may decide to also test / verify the identified skills (if desired) in a practical manner also in the case of Roles identified in e-Competence levels 1 (although not mandatory).

2.4. Open questions

This deliverable, aims to continue on the path of the CONCORDIA Cybersecurity Skills Certification Framework and address the points not fully analyzed. Specifically, the points that appear to bear analysis and recommendations are the following:

- Which is the e-competency proficiency level of each one of the skills and knowledge of the 12 Role Profiles included in the ECSF (European Cybersecurity Skills Framework)⁸?
- Which are the categories into which the cybersecurity skills could be assigned to (with an aim to correlated them to appropriate assessment methods)?
- Which are the different methods that knowledge of different proficiency levels could be assessed?
- Which could be possible practical assessment methods of cybersecurity skills?

The rest of this document is structured in a way that addresses each one of the above questions in sequence.

3. Proficiency levels

In deliverable R3.3.1. Cybersecurity Skills Framework⁹ the results of the analysis of each of the 12 roles introduced within the ECSF (at the time of publication 0.5 draft version) are depicted.

Amongst others, these results contain tables (as an example see Figure 1. Chief Information Security Officer (CISO) below) that depict the identified e-competencies (M= Mandatory and O= Optional) of the role and for each the desirable proficiency level based on the e-cf¹⁰.

⁸ <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>

⁹ <https://rewireproject.eu/results/>

¹⁰ European e-Competence Framework 3.0 User guide for the application of the European e-Competence Framework 3.0. CWA 16234:2014 Part 2. © CEN

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	

Figure 1. The analysis of the e-competencies of the CISO



To further understand the knowledge and skills included within each one of these e-competencies and the proficiency level to which they should be acquired by an individual, the analysis (again as part of R3.3.1.) was extended to match the tasks of the role to the required knowledge, skills and e-competencies. This analysis was decided upon taking into consideration the basic definition of the Role Profiles (see Section 2.1), which in summary says that knowledge, skills and e-competencies are needed in order to effectively undertake the tasks of the role.

Due to the volume of the results of this analysis, below an example is provided only for a few tasks of the role of the Chief Information Security Officer (CISO) and the Cybersecurity Risk Manager¹¹. In each case, the example starts with the description of the task and is followed by the identified Knowledge, Skills and e-competencies. Then for each case the proficiency level of each is identified and explained.











Chief Information Security Officer (CISO)

Task 1: 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.












Relevant **Knowledge:**

-  Knowledge of critical threats, vulnerabilities and controls for the organisation's information provision
-  Knowledge of cybersecurity maturity models





¹¹ Through the selection of the specific roles, we have the ability to provide information on all e-cf proficiency levels.

-  Knowledge of enterprise architecture
-  Knowledge of organisation's overall ICT infrastructure and key components
-  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 security approach in information strategy of the organisation
-  Knowledge of security controls frameworks and standards
-  Knowledge of cybersecurity-related legislation, policies, regulations, standards, certifications and best practices
-  Understand core organisational business processes
-  Knowledge of data protection and data privacy legislation, policies and regulations
-  Knowledge of the hierarchy of documentation (policies, procedures, standards, guidelines etc)

Relevant Skills:

-  Understand core organisational business processes
-  Understand the results of assessments and the possible impact of findings & interpret security analytics
-  Understand, analyse and implement cybersecurity management, design and document the processes for risk analysis and management
-  Understand, analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications and best practices
-  Review and enhance security documents, reports, SLAs and ensure the security objectives
-  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.
-  Apply relevant standards, best practices and legal requirements for information security
-  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
-  Establish a cybersecurity plan

Relevant e-competencies:

- | | | |
|---|--|---------|
|  | A.1. Information Systems and Business Strategy Alignment | Level 5 |
|  | A.2. Service Level Management | Level 4 |
|  | D.1. Information Security Strategy Development | Level 5 |
|  | E.8. Information Security Management | Level 4 |

The above show that the Skills related to

- A.1. Information Systems and Business Strategy Alignment
- D.1. Information Security Strategy Development need to be at the highest level (Level 5 of the e-cf).

Based on the information provided within the e-Cf, e-CF level e-5, the Principal, has overall accountability and responsibility; is recognized inside and outside the organization for innovative solutions and for shaping the future using outstanding leading edge thinking and knowledge. It should be noted that this level corresponds to the 8th EQF^{12, 13} level which has the following description:

Knowledge	Skills	Responsibility and autonomy
Knowledge at the most advanced frontier of a field of work or study and at the interface between fields	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	Demonstrate substantial authority, innovation, autonomy, scholarly and professional integrity and sustained commitment to the development of new ideas or processes at the forefront of work or study contexts including research

Table 2. Learning outcomes of Level 8 - EQF

Whereas,

- A.2. Service Level Management
- E.8. Information Security Management need to be at Level 4 of the e-cf.

Based on the information provided within the e-Cf, e-CF level e-4, the Lead Professional / Senior manager, has extensive scope of responsibilities deploying specialized integration capability in complex environments; full responsibility for strategic development of staff working in unfamiliar and unpredictable situations. It should be noted that this level corresponds to the 7th EQF level which has the following description:

¹² <https://europa.eu/europass/en/description-eight-efq-levels>

¹³ The European Qualifications Framework (EQF) is a common European reference framework whose purpose is to make qualifications more readable and understandable across different countries and systems. Covering qualifications at all levels and in all sub-systems of education and training, the EQF provides a comprehensive overview over qualifications in the 38 European countries currently involved in its implementation. <https://www.cedefop.europa.eu/en/projects/european-qualifications-framework-efq>

Knowledge	Skills	Responsibility and autonomy
Highly specialised knowledge, some of which is at the forefront of knowledge in a field of work or study, as the basis for original thinking and/or research Critical awareness of knowledge issues in a field and at the interface between different fields	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	Manage and transform work or study contexts that are complex, unpredictable and require new strategic approaches; take responsibility for contributing to professional knowledge and practice and/or for reviewing the strategic performance of teams











Table 3. Learning outcomes of Level 7 - EQF

Task 2: Design, develop, implement, manage and continually improve the information security management system.

Relevant Knowledge:

 Knowledge of cybersecurity maturity models.

Relevant Skills:

-  Understand core organisational business processes
-  Understand the results of assessments and the possible impact of findings & interpret security analytics
-  Understand, analyse and implement cybersecurity management, design and document the processes for risk analysis and management
-  Understand, analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications and best practices
-  Review and enhance security documents, reports, SLAs and ensure the security objectives
-  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.
-  Apply relevant standards, best practices and legal requirements for information security
-  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

Relevant e-competencies:

- A.6. Application Design Level 1
- A.5. Architecture Design Level 3
- B.3. Testing Level 1

☒ C.5. Systems Management

Level 1

The above show that the Skills related to

A.6. Application Design

B.3. Testing

C.5. Systems Management need to be at the Level 1 of the e-cf.

Based on the information provided within the e-Cf, e-CF level e-1, the Associate, is able to apply knowledge and skills and solve straight forward problems; is responsible for own actions and is operating in a stable environment. It should be noted that this level corresponds to the 3th EQF level which has the following description:

Knowledge	Skills	Responsibility and autonomy
Knowledge of facts, principles, processes and general concepts, in a field of work or study	A range of cognitive and practical skills required to accomplish tasks and solve problems by selecting and applying basic methods, tools, materials and information	Take responsibility for completion of tasks in work or study; adapt own behavior to circumstances in solving problems

Table 4. Learning outcomes of Level 3 - EQF

Whereas,

A.5. Architecture Design need to be at Level 3 of the e-cf.

Based on the information provided within the e-Cf, e-CF level e-3, the Senior Professional / Manager, is respected for innovative methods and use of initiative in specific technical or business areas; is providing leadership and taking responsibility for team performances and development in unpredictable environments. It should be noted that this level corresponds to the 6th EQF level which has the following description:


Knowledge	Skills	Responsibility and autonomy
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 specialised field of work or study	Manage complex technical or professional activities or projects, taking responsibility for decision-making in unpredictable work or study contexts; take responsibility for managing professional development of individuals and groups

Table 5. Learning outcomes of Level 6 - EQF



Cybersecurity Risk Manager

Task 1: Knowledge of critical threats, vulnerabilities and controls for the organization.






Relevant Knowledge:

-  Knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices

Relevant Skills:

-  Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards
-  Analyse and consolidate organisation’s quality and risk management practices

Relevant e-competencies:

-  B.5. Documentation Production Level 2
-  D.1. Information Security Strategy Development Level 5
-  E.3. Risk Management Level 4
-  E.8. Information Security Management Level 3
-  E.9. IS-Governance Level 4

The above show that the Skills related to

B.5. Documentation Production need to be at the Level 2 of the e-cf.

Based on the information provided within the e-Cf, e-CF level e-3, the Professional, operates with capability and independence in specified boundaries and may supervise others 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. It should be noted that this level corresponds to the 4th and 5th EQF level which has the following description:

Knowledge	Skills	Responsibility and autonomy
Comprehensive, specialised, factual and theoretical knowledge within a field of work or study and an awareness of the boundaries of that knowledge	A comprehensive range of cognitive and practical skills required to develop creative solutions to abstract problems	Exercise management and supervision in contexts of work or study activities where there is unpredictable change; review and develop performance of self and others
Factual and theoretical knowledge in broad contexts within a field of work or study	A range of cognitive and practical skills required to generate solutions to specific problems in a field of work or study	Exercise self-management within the guidelines of work or study contexts that are usually predictable, but are subject to change; supervise the routine work of others, taking some responsibility for the evaluation and improvement of work or study activities

Table 6. Learning outcomes of Level 5 and 4 - EQF

Figure 2. provides an overall overview of all the levels referred to above for the European e-CF and EQF. Beside of concepts explicitly elaborated for the European e-Competence Framework, the table contains description elements of 1) The European Qualifications Framework for Lifelong Learning (EQF), April 2008 and 2) The PROCOM Framework, of which generic job titles have been reproduced by kind permission of e-Skills UK.¹⁴

3.1. Topics to consider when deciding tasks

The skills needed for each profile described in R3.3.1 Cybersecurity skills Framework¹⁵ are intertwined with several intersections. The following are some of the fundamental skills needed across various profiles:

- Cryptography. Knowledge in cryptography entails developing security systems using ciphers and algorithms to encrypt sensitive data, preventing misuse. This can also include protecting data from being decrypted, altered, copied or modified in any way by an exploiter. Since the emergence of cloud technologies and financial technologies, cryptography is a vital skill for many profiles.
- Network configuration is the process of setting up a network's policies, traffic flows, settings, controls. With the rise of virtualization and automation, an optimally setup network is vital for scalability, efficiency and security.
- Network security tools in continuation to the previous point. Networks are growing at an exponential pace. This has attracted a lot of malicious users and an increase in various network attacks like DDoS, man in the middle attacks etc. Mastering the use of network tools and techniques to secure a network is critical. This includes tasks like setting up network honey pots, network intrusion detection systems, good firewall policies, network Identity management systems etc.
- Traffic Analysis. This is the process of making sense of network traffic captures. Traffic analysis is central to several job profiles. Sheds light on the step by step process by which a network attack was carried out. It can also provide details on the compliance of network devices, network policy and the user behavior.
- Web API exploitation. This involves the hostile use of a publicly exposed web API. A knowledge of DDoS attacks, authentication hijacking, Man in the middle, data exposure and parameter modification is required for this skill.
- Digital forensics

¹⁴[User-guide-for-the-application-of-the-e-CF-3.0 CEN CWA 16234-2 2014.pdf](https://itprofessionalism.org/user-guide-for-the-application-of-the-e-CF-3.0-CEN-CWA-16234-2-2014.pdf)
(itprofessionalism.org)

¹⁵ https://rewireproject.eu/wp-content/uploads/2022/11/R3.3.1.-Cybersecurity-Skills-Framework_FINAL.pdf

EQF levels	EQF Levels descriptions	e-CF Levels	e-CF Levels descriptions	Typical Tasks	Complexity	Autonomy	Behaviour
8	Knowledge at the most advanced frontier, the most advanced and specialised skills and techniques to solve critical problems in research and/or innovation, demonstrating substantial authority, innovation, autonomy, scholarly or professional integrity.	e-5	Principal Overall accountability and responsibility; recognised inside and outside the organisation for innovative solutions and for shaping the future using outstanding leading edge thinking and knowledge.	IS strategy or programme management	Unpredictable – unstructured	Demonstrates substantial leadership and independence in contexts which are novel requiring the solving of issues that involve many interacting factors.	Conceiving, transforming, innovating, finding creative solutions by application of a wide range of technical and/or management principles.
7	Highly specialised knowledge, some of which is at the forefront of knowledge in a field of work or study, as the basis for original thinking, critical awareness of knowledge issues in a field and at the interface between different fields, specialised problem-solving skills in research and/or innovation to develop new knowledge and procedures and to integrate knowledge from different fields, managing and transforming work or study contexts that are complex, unpredictable and require new strategic approaches, taking responsibility for contributing to professional knowledge and practice and/or for reviewing the strategic performance of teams.	e-4	Lead Professional / Senior Manager Extensive scope of responsibilities deploying specialised integration capability in complex environments; full responsibility for strategic development of staff working in unfamiliar and unpredictable situations.	IS strategy/ holistic solutions		Demonstrates leadership and innovation in unfamiliar, complex and unpredictable environments. Addresses issues involving many interacting factors.	
6	Advanced knowledge of a field of work or study, involving a critical understanding of theories and principles, advanced skills, demonstrating mastery and innovation in solving complex and unpredictable problems in a specialised field of work or study, management of complex technical or professional activities or projects, taking responsibility for decision-making in unpredictable work or study contexts, for continuing personal and group professional development.	e-3	Senior Professional / Manager 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.	Consulting	Structured – unpredictable	Works independently to resolve interactive problems and addresses complex issues. Has a positive effect on team performance.	Planning, making decisions, supervising, building teams, forming people, reviewing performances, finding creative solutions by application of specific technical or business knowledge/skills.
5	Comprehensive, specialised, factual and theoretical knowledge within a field of work or study and an awareness of the boundaries of that knowledge, expertise in a comprehensive range of cognitive and practical skills in developing creative solutions to abstract problems, management and supervision in contexts where there is unpredictable change, reviewing and developing performance of self and others.	e-2	Professional Operates with capability and independence in specified boundaries and may supervise others 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.	Concepts/ Basic principles		Works under general guidance in an environment where unpredictable change occurs. Independently resolves interactive issues which arise from project activities.	
4	Factual and theoretical knowledge in broad contexts within a field of work or study, expertise in a range of cognitive and practical skills in generating solutions to specific problems in a field of work or study, self-management within the guidelines of work or study contexts that are usually predictable, but are subject to change, supervising the routine work of others, taking some responsibility for the evaluation and improvement of work or study activities.				Structured – predictable	Scheduling, organising, integrating, finding standard solutions, interacting, communicating, working in team.	
3	Knowledge of facts, principles, processes and general concepts, in a field of work or study, a range of cognitive and practical skills in accomplishing tasks. Problem solving with basic methods, tools, materials and information, responsibility for completion of tasks in work or study, adapting own behaviour to circumstances in solving problems.	e-1	Associate Able to apply knowledge and skills to solve straight forward problems; responsible for own actions; operating in a stable environment.	Support/ Service	Structured – predictable	Demonstrates limited independence where contexts are generally stable with few variable factors.	Applying, adapting, developing, deploying, maintaining, repairing, finding basic-simple solutions.

Figure 2. EQF, e-cf and PROCOM levels

4. Assessment methods

4.1. Assessment of cybersecurity knowledge

As mentioned in Section 2.1. Knowledge is the “Body of facts, principles, theories and practices that is related to a field of work or study. Knowledge is a body of information applied directly to the performance of a function.”

In STANDARDS for Educational and Psychological Testing by the American Educational Research Association, the American Psychological Association, and the National Council on Measurement in Education, 2014, the following definitions regarding test are provided:

A test is an evaluative device or procedure in which a systematic sample of a test taker’s behavior in a specified domain is obtained and scored using a standardized process.

The following types of tests are identified:

- achievement test** : A test to measure the extent of knowledge or skill attained by a test taker in a content domain in which the test taker has received instruction.
- adaptive test** : A sequential form of individual testing in which successive items, or sets of items, in the test are selected for administration based primarily on their psychometric properties and content, in relation to the test taker’s responses to previous items.
- mastery test** : A test designed to indicate whether a test taker has attained a prescribed level of competence, or mastery, in a domain.
- job sample test** : A test of the ability of an individual to perform the tasks comprised by a job.

“A test is a device or procedure in which a sample of an examinee’s behavior in a specified domain is obtained and subsequently evaluated and scored using a standardized process.”¹⁶

Tests differ on a number of dimensions:

- ⇒ the mode in which test materials are presented (e.g., paper-and-pencil, oral, or computerized administration);
- ⇒ the degree to which stimulus materials are standardized;
- ⇒ the type of response format (selection of a response from a set of alternatives, as opposed to the production of a free-form response); and
- ⇒ the degree to which test materials are designed to reflect or simulate a particular context.

In relation to the type of response format and the type of tests that could be implemented to assess knowledge, W. James Popham Professor Emeritus, University of California, Los Angeles

¹⁶ Hogan, T. P. (2007). Psychological testing, A practical introduction (2nd ed.). Retrieved from The University of Phoenix eBook Collection database.

in Classroom Assessment. What Teachers Need to Know, Eighth edition. 2017, provides the following information:

- ❑ Binary-choice items: A binary-choice item gives students only two options from which to select. The most common form of binary-choice item is the true–false item. Other variations of binary-choice items would be those in which students must choose between yes–no, right–wrong, correct–incorrect, fact–opinion, and so on.
- ❑ Multiple binary-choice items: A multiple binary-choice item is one in which a cluster of items is presented to students, requiring a binary response to each of the items in the cluster. Typically, but not always, the items are related to an initial statement or set of statements. Multiple binary-choice items are formatted so they look like traditional multiple-choice tests. In a multiple-choice test, the student must choose one answer from several options, but in the multiple binary-choice test, the student must make a response for each statement in the cluster.
- ❑ Multiple-choice items: Multiple-choice items can be used to measure a student’s possession of knowledge or a student’s ability to engage in higher levels of thinking. A strength of multiple-choice items is they can contain several answers differing in their relative correctness. Thus, the student can be called on to make subtle distinctions among answer options, several of which may be somewhat correct. A weakness of multiple-choice items, as is the case with all selected-response items, is that students need only recognize a correct answer. Students need not generate a correct answer. Although a fair amount of criticism has been heaped on multiple-choice items, particularly in recent years, properly constructed multiple-choice items can tap a rich variety of student skills and knowledge, and thus can be useful tools for classroom assessment.
- ❑ Matching items: A matching item consists of two parallel lists of words or phrases requiring the student to match entries on one list with appropriate entries on the second list. Entries in the list for which a match is sought are referred to as premises. Entries in the list from which selections are made are referred to as responses. Usually, students are directed to match entries from the two lists according to a specific kind of association described in the test directions.
- ❑ Short-answer items: These types of items call for students to supply a word, a phrase, or a sentence in response to either a direct question or an incomplete statement. If an item asks students to come up with a fairly lengthy response, it would be considered an essay item, not a short-answer item. If the item asks students to supply only a single word, then it’s a really short-answer item. Short-answer items are suitable for assessing relatively simple kinds of learning outcomes such as those focused on students’ acquisition of knowledge. If crafted carefully, however, short-answer items can measure substantially more challenging kinds of learning outcomes. The major advantage of short-answer items is that students need to produce a correct answer, not merely recognize it from a set of selected-response options.
- ❑ Essay items: The essay item is surely the most commonly used form of constructed-response assessment item. Anytime teachers ask their students to churn out a paragraph or two on what the students know about Topic X or to compose an original composition describing their “Favorite Day,” an essay item is being used. Essay items

are particularly useful in gauging a student's ability to synthesize, evaluate, and compose.

- ❑ Observational approaches: More often than not, an examiner (such as the teacher) observes the process of construction so that observation of the student's performance and judgment of that performance are required.
- ❑ Portfolios: A portfolio is a systematic collection of one's work. In education, portfolios refer to systematic collections of students' work. Although the application of portfolios in education has been a relatively recent phenomenon, portfolios have been widely used in a number of other fields for many years. Portfolios, in fact, constitute the chief method by which certain professionals display their skills and accomplishments.
- ❑ Affective assessment procedures: Affective variables, most educators concede, are important. Students' attitudes toward learning, for example, play a major role in how much learning those students subsequently pursue. The values students have regarding truthfulness and integrity shape their daily conduct. And students' self-esteem, of course, influences almost everything they do. There's little doubt that the affective status of students should concern all educators

During the design of each assessment, the different characteristics of the above-mentioned test types should be taken into consideration along with the type of knowledge being assessed and the level this knowledge should be assessed at.

For example, as mentioned in Section 3, for a person to be able to effectively implement the Task: 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, that person needs to have "Knowledge of the hierarchy of documentation (policies, procedures, standards, guidelines etc)" at a high level.

This means that the type of test items and methods should be appropriate to that level e.g. most probably Binary choice items will not be used as part of the assessment process.

4.2. Assessment of cybersecurity skills

As mentioned in Section 2.1 above, a skill is defined as "The ability to use know-how and expertise to complete tasks and solve problems. 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."

Since a cybersecurity skill is related with the ability to perform a specific task, the method and tools that used to assess its presence, should also be able to show that the ability exists. This means, that most of the methodologies of tests presented in Section 4.1 cannot be used.

The assessment methods for cybersecurity skills should be able to allow the candidate to show that that they have the ability to perform the task, in a realistic environment using the adequate tools to solve specific challenges.

Furthermore, it should have a grade scale from simple to complex assessments, based on the specific skills being evaluated and the grade of competence of the candidate. Some people are strong on education; others are rich in experience. Skills assessment tests give no weight to how employees learned what they know; they measure what employees can do. In general, there are three types of skills:

- **Functional skills** are used to accomplish a task. These skills require the candidate to perform a series of actions(s) in order to achieve some tangible result.
- **Attitude management skills** are less tangible, but complement functional skills. They help achieve tasks with greater trust and efficiency. The right attitude is important in cybersecurity since a majority of tasks will entail working ethically in a high stress, time bound environment.
- **Knowledge based** skills are all the information a candidate needs to achieve a certain task. This includes, knowledge on certain procedures, theory and operation of specific subjects in cybersecurity.

The next section will analyse the various type of exercises used to assess a person's skill.

4.2.1. Theory on practical cybersecurity skills assessment

An exercise consists of various tasks. These tasks have to be completed in order to finish an exercise. Depending on the skills being assessed, a different combination of tasks of varying difficulty can be chosen when creating an exercise. Furthermore, several types of exercises can be used to evaluate a candidates Cybersecurity skill and the selection (design) depends on the type and difficulty of the skill being assessed. For example, in order to assess more advanced skills multiple challenges can be combined with the addition of a constraint of time or live adversaries.

4.2.2. Multiple choice questions approach^{17 18}

Multiple choice questions are those questions that are posed alongside a list of possible answers. Typically, these have three to four answers that the candidate may select from. Multiple-choice questions enjoy wide applicability and acceptance. They come in 2 main formats:

- The single multiple-choice question, where out of a list of answers only a single correct has to be selected.
- The multi-select multiple choice question, where multiple options in the list of answers can be true.

Multiple choice questions can be used to evaluate skills of varying levels, with multi-select multiple choice question being used for higher level skills.

It should be noted that multiple choice questions is a method of validating that a candidate is in possession of a specific knowledge (as already mentioned Section 4.1). This method can

¹⁷ Ding, L., & Beichner, R. (2009). Approaches to data analysis of multiple-choice questions. *Physical Review Special Topics-Physics Education Research*, 5(2), 020103.

¹⁸ Considine, J., Botti, M., & Thomas, S. (2005). Design, format, validity and reliability of multiple choice questions for use in nursing research and education. *Collegian*, 12(1), 19-24.

be used also, in the case of skills if expressed correctly. I.e., The multiple-choice questions that aim to assess skills, would present the participant with questions that require the combination of the specific knowledge (**Knowledge based skills**) in order to complete a task or would present a scenario which the candidate would be requested to follow understand and solve. This type of assessment is recommended to be used for the lower proficiency levels (e.g. Levels 1-2).

The following figures depict the appropriateness of this assessment method to the different proficiency levels of the EQF and the e-CF as mentioned in 3.

EQF levels	1 ✓	2 ✓	3	4	5	6	7	8
------------	-----	-----	---	---	---	---	---	---

- 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 levels	1 ✓	2 ✓	3	4	5
-------------	-----	-----	---	---	---

- 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.

4.2.3. A simulation based approach¹⁹

Cybersecurity roles require configuring, analyzing and debugging large Cyber environments. However, access to physical devices can be difficult due to a large number of resources needed. Instead, simulation-based assessments are used as an alternative. In simulation-based assessment a sandbox environment is setup with several emulated devices (these devices can potentially be running the same software stack as physical hardware), the candidate has to address a deficiency in the simulated environment by either fixing a fault, setting up new services and/or analyzing/recovering information in the sandbox. Simulation based evaluation are a great way of studying if a candidate understands all the tools at his/her disposal, analyze the root cause of a problem and most importantly understand how each component of a system functions and interacts. The following are a few exercise types that can be setup on simulators.

¹⁹ Crellin, Jonathan & Adda, Mo & Duke-Williams, Emma. (2010). The use of simulation in digital forensics teaching.

4.2.3.1. Forensics Analysis

Examples of forensics analysis simulations are:

- Seizure simulations and
- Forensic house simulations.

Seizure simulations involve presenting the candidate with an environment that contains sensitive data. The challenge is to extract the data in a forensically safe way. For example, shutting down a computer normally can result in the loss of critical evidence because it increases disk activity. Or it could involve breaking cryptography ciphers to access hidden data. These types of simulations are generally easier to setup, require knowledge of low-level processes within a system and could be used for a candidate to exhibit the successful performance of a task and the understanding of the underlying principles.

The forensic house simulations are simulated crime scenes that are used to support a variety of forensic disciplines. Such simulation could depict compromised network right after an attack where the candidate has to investigate the parameters of the attack or identify compromised devices etc. The setup involved in these types of simulations are more difficult involving larger number of devices and could be used to access that a candidate can perform tasks in an unpredictable way, combining the knowledge and skills already possessed.

4.2.3.2. Setup and debugging simulations

Setup simulations are used to assess if a candidate has the skill and know how in configuration and running a cyber security system. This can include tuning various parameters, ensuring the adequate security policies are in place. For example, setting up a network wide intrusion detection system involves selecting the models, network traffic sampling procedures and deciding analysis and action routines. This assessment can also be used to test the fundamentals of a network knowledge such as how packet routing takes place or how capture traffic and perform analysis.

Debugging involves identifying a problem, isolating the root cause and then fixing or proposing a workaround. This can include be a badly configured device, a compromised system or faulty equipment. An aptitude for debugging can also help in several other fields like forensics and penetration testing. Debugging assessments can be performed by setting up a nonfunctioning sand box and asking the candidate to fix the problem.

Several fields of Cybersecurity like cryptography and reverse engineering do not require the need for expensive virtual environments. **Do it yourself problems**, can be provided as written text with the student having to install all the relevant tools. "Cryptopals"²⁰ is one such example of a set of problems aimed at educating on cracking ciphers. Students only need to have access to a python interpreter. The problem set provides detailed description on approach, methodology and theory wherever needed. This style also encourages students to develop tools themselves like functions to extract fields using Scapy²¹ or to convert between various formats like base64 or Hex etc.

²⁰ <https://cryptopals.com/>

²¹ <https://scapy.net/>

Penetration testing or pen testing is a simulated attack on a computer system performed to access the security. This generally involves 5 steps, planning, scanning, gaining access, keeping access and analysis. A sandbox environment can be setup with candidates trying to get root access to a system, bypass a security or identify various vulnerabilities in the system. This is very similar to a gamified approach except it happens in a noncompetitive environment where candidates have more time and are not penalized as much.

The following figures depict the appropriateness of this assessment method to the different proficiency levels of the EQF and the e-CF as mentioned in 3.

EQF levels	1 ✓	2 ✓	3 ✓	4 ✓	5 ✓	6 ✓	7	8
------------	-----	-----	-----	-----	-----	-----	---	---

- 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 levels	1 ✓	2 ✓	3 ✓	4	5
-------------	-----	-----	-----	---	---

- 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.

4.2.4. A Gamified approach

In Cybersecurity Skills Training: An Attacker-Centric Gamified Approach Mackenzie Adams and Maged Makramalla conclude that “Based on our review of the literature, we propose a gamified approach to cybersecurity skills training. Using the elements of gamification, we outline four components required to create a comprehensive cybersecurity skills training: i) story, ii) player control, iii) problem solving, and iv) progress mechanics.”

Gamification is a process of enhancing a specific service by implementing game design elements in a non-game context to enhance the user’s overall value creation and experience^{22, 23}. Deterding and colleagues define gamification as “the use of design elements characteristic for games in non-game contexts”. Thus, gamification reflects the use

²² Huotari, K.; Hamari, J. Gamification from the Perspective of Service Marketing. In Proceedings of the CHI 2011 Workshop Gamification, Vancouver, BC, Canada, 7–12 May 2011.

²³ Deterding, Sebastian & Dixon, Dan & Khaled, Rilla & Nacke, Lennart. (2011). From Game Design Elements to Gamefulness: Defining Gamification. Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, MindTrek 2011. 11. 9-15. 10.1145/2181037.2181040.

of game thinking including progress mechanics (such as points systems), player control (such as avatar use), rewards, collaborative problem solving, stories, and competition in non-game situations²⁴. Underlying gamification is an understanding of motivation as significantly correlated with and predictive of desirable human outcomes such as achievement, success, and the attainment of distinction and rewards²³. When designed and applied in an appropriate manner and setting, gamification provides an alignment between motivation and desire that leads to the anticipated purpose of its use. For instance, when used to increase employee engagement, gamification can improve teamwork and transform routine, often dull, tasks by motivating employees through "play" and competition within the same team and across teams^{25,26}. Although it is usually considered an effective user involvement tool, gamification can also be used to develop skills of participants and employees. Burke²⁷ highlights the effectiveness of using gamification concepts in employee training while using the "Ignite Leadership Game" created by NTT Data as a relevant example. This specific gameful design is built on first assessing the employees' knowledge to identify their strengths and weaknesses; the identification allows them to develop the required skill sets more efficiently. The main benefits of using gamification approaches to develop skills are creating an atmosphere that enables employee active involvement²⁸, improving the participants' motivation to achieve better results²⁹, and enhancing the overall learning process due to the established collaborative environment²⁸.

There are various types of exercises / activities that incorporate this gamification element within the cybersecurity domain. Specifically,³⁰:

Cybersecurity game: A serious game is a software application that uses computer game structure or includes game elements for a primary purpose other than entertainment, such as for learning, practicing, or competing. A cybersecurity game is a serious game designed to apply cybersecurity concepts. Note that a cybersecurity game differs from a cybersecurity exercise, which is a simulated training event. ISO 22398:2013³¹ defines the terms related to (cybersecurity) exercises.

Capture the flag (CTF): Originally, *Capture the flag* is a traditional outdoor game for two teams. Each team has one physical flag in their base. The goal is stealing the other team's flag and bringing it to own base, while at the same time defending the own flag. Popular computer games, such as World of Warcraft or Team Fortress 2, also use this structure. In this work, CTF is a specific cybersecurity game. To define it

²⁴ Kapp, Karl. (2012). The gamification of learning and instruction: Game-based methods and strategies for training and education. San Francisco, CA: Pfeiffer.

²⁵ Korolov, M. (2012). Gamification of the Enterprise. Network World, 9(2012), 31-33.

²⁶ Zichermann, G., & Cunningham, C. (2011). Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps. Sebastopol, CA: O'Reilly Media.

²⁷ Burke, B. (2016). Gamify: How gamification motivates people to do extraordinary things: Routledge.

²⁸ The Gamification Revolution: How Leaders Leverage Game Mechanics to Crush the Competition, Gabe Zichermann, Joselin Linder. 2013

²⁹ Gamify How Gamification Motivates People to Do Extraordinary Things By Biran Burke. 2014. 1st Edition.

³⁰ Masaryk University, Faculty of Informatics, Prerequisite testing of cybersecurity skills, master's Thesis, Bc. Valdemar Švábenský

³¹ <https://www.iso.org/standard/50294.html>

precisely, CTFtime³² an archive and a roadmap for these games, lists three types of CTFs: Attack-defense, Jeopardy, and a mix of these two.

Attack-defense CTF: In an Attack-defense CTF, each team (having one or more players) controls a computer network with hosts running vulnerable services. The goal is attacking other teams’ assets and stealing secret information: flags (usually long random strings), while at the same time defending the own assets. The teams normally receive time to prepare their exploits and patches in advance. Historically, Attack-defense is the first type of CTF games, and some authors³³³⁴³⁵ use the term CTF to mean Attack-defense CTF exclusively. Attack-only or Defense-only CTFs may be viewed as a subcategory. Still, there is no clear line between attacking and defending^{36,19}, since offensive and defensive skills are closely related. Some suggest that learning to attack is required for learning to defend²², for example, finding a security flaw in a program is the first step to repairing it.

Jeopardy CTF: In a Jeopardy CTF, each team (having one or more players) receives several tasks. The task topics are similar to Attack-defense CTFs and include web security, service exploitation, cryptography, network forensics, or reverse engineering. Since the tasks are usually of an offensive nature, Jeopardy CTFs can be regarded as a subcategory of Attack-only CTFs³⁷. However, this text makes a distinction: the tasks in Attack defense CTFs are carried out in an underlying network infrastructure; in Jeopardy CTFs, the tasks are often simply predefined in a web interface or a virtual machine. Completing a task yields a unique flag confirming the solution; the tasks’ difficulty and score value gradually increase.

The following figures depict the appropriateness of this assessment method to the different proficiency levels of the EQF and the e-CF as mentioned in 3.



- 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.

³² CTFtime. CTFtime.org / All about CTF (Capture The Flag). <https://ctftime.org/ctf-wtf/> (accessed October 2022)

³³ Martin Mink and Rainer Greifeneder. Evaluation of the Offensive Approach in Information Security Education. In Security and Privacy – Silver Linings in the Cloud, volume 330 of IFIP Advances in Information and Communication Technology, pages 203–214. Springer, 2010.

³⁴ Jelena Mirkovic and Peter A. H. Peterson. Class Capture-the-Flag Exercises. In 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), San Diego, CA, 2014. USENIX Association.

³⁵ Giovanni Vigna. Red Team/Blue Team, Capture the Flag, and Treasure Hunt: Teaching Network Security Through Live Exercises. In In World Conference on Information Security Education, 2003.

³⁶ Mark Gondree, Zachary Peterson, and Portia Pusey. Talking about cybersecurity games. USENIX ;login;, 41(1):36–39, 2016.

³⁷ Andy Davis, Tim Leek, Michael Zhivich, Kyle Gwinnup, and William Leonard. The Fun and Future of CTF. In 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), San Diego, CA, 2014. USENIX Association

- 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.

4.2.5. Other types of exercises

Onsight internships are another strategy that helps evaluate a person’s skills in a working environment. It provides a mechanism for the industry to evaluate if the cumulative skills acquired are appropriate for what is needed in the industry. It also helps identify several soft skills like task management, communication and teamwork. Furthermore, it helps transfer knowledge about industry specific norms that are not accessible in the classroom. Employer feedback is important for evaluating a student and identifying what areas further training is required.

4.2.6. Cyber ranges as an assessment platform

The WG5 PAPER, Understanding Cyber Ranges: From Hype to Reality, SWG 5.1 | Cyber Range Environments and Technical Exercises, MARCH 2020, introduces the subject of cyber ranges, provides one common definition and presents the use case of cybersecurity skills assessment for cyber ranges. Specifically:

What is a Cyber Range?

The meaning of cyber ranges has changed over the years and so has the way they have been defined. A review of currently existing definitions and interpretations from around the world from both private and public sector cyber range initiatives broadly identifies two possible ways of defining a cyber range:

A simulation environment – This view of the cyber range focuses on what cyber ranges have traditionally provided, which is a simulation of ICT and/or OT environments to be used for a wide set of purposes. Some definitions look at cyber ranges as inclusive of the Internet services, which are connected to the simulated environment. This way of defining cyber ranges is somewhat static as it usually refers to a simulation environment which is designed once to meet specific use cases and requirements and where any change in the environment requires considerable time and effort.

A platform – A platform is usually defined as a group of technologies that are used as a base upon which other applications, processes or technologies are developed. In the context of cyber ranges, a platform can be intended to be a group of technologies that are used to create and use a simulation environment. The emphasis here is on the word “use” since for a cyber range to be used for specific purposes, the cyber range must have additional capabilities and expose specific functionalities to the end user. This view of the cyber range is clearly more dynamic as it implies that different environments can be more easily created and that functionalities are provided to help in the use of the simulation environment. How easy it is to dynamically create different simulation environments and the breadth of functionalities offered will then vary across different cyber ranges.

NIST’s definition, for instance, falls into the first interpretation of what a cyber range is, making no reference to services and/or functionalities to be provided by a cyber range other than the simulation environment [5]:

“interactive, simulated representations of an organization’s local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing. A cyber range may include actual hardware and software or may be a combination of actual and virtual components. Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer.

In the deliverable R4.1.1 - Cyber Range Establishment methodology and roadmap, there is a definition of a Cyber Range according to the REWIRE project. “A Cyber Range is an environment where situational operations training, testing, research, and educational development can be performed. Therefore, the scope of Cyber Ranges is not only limited to organizations and professionals but also students and educational entities. The technology utilized for the creation of such environments is vast and it can be hardware, software, or a combination of both. This environment is closed and risk-free which allows real-life scenarios to take place. Gaining hands-on skills, testing services or products, and performing security testing are the main use cases for Cyber Ranges.

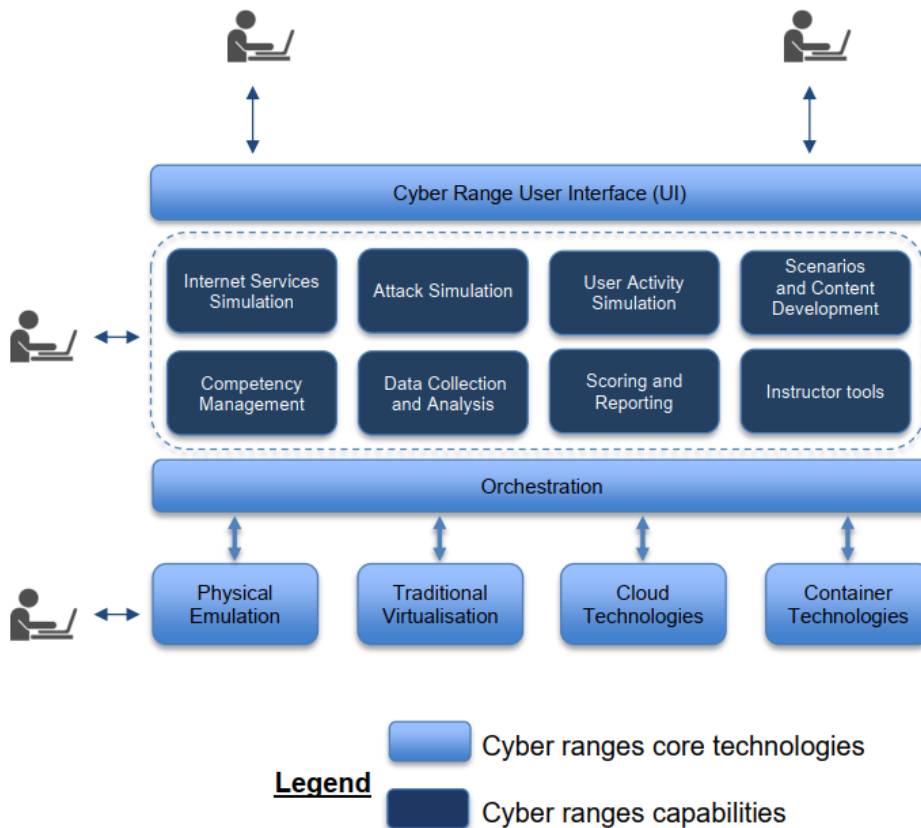


Figure 3. Sample Architectural Components of a Cyber Range³⁸

5. Conclusions

This document describes the various methods that can be used for the assessment of Cybersecurity Knowledge and Skills.

As depicted by the relevant information (Section 4.1), the methods that can be used for the assessment of Cybersecurity Knowledge can be “theoretical” (static items), differing in way that the items are designed, the type and complexity of the items and the type of response format. The items shall be designed taking into consideration the level of knowledge required E.g. The ECSF defines that for the effective performance of the role of the Cyber Threat Intelligence Specialist, “Advanced knowledge of cybersecurity solutions, outputs and integrity to comprehensive cybersecurity concept” should be possessed by the individual, the items need to be designed in such a way that advanced knowledge is proven.³⁹

On the subject of assessment of cybersecurity knowledge, this recommendation subscribes to the requirement for Theoretical assessment as depicted within the CONCORDIA Cybersecurity Skills Certification Framework, with the addition that the complexity of questions shall be designed based on the level of knowledge prescribed by the profile description⁴⁰.

³⁸ Deliverable R4.1.1 - Cyber Range Establishment methodology and roadmap

³⁹ This would most probably mean that the items would not be restricted to basic definitions but would cover also more advanced and detailed knowledge.

⁴⁰ In the C³ by CONCORDIA certification scheme, a rule has been set for the number of easy, medium or hard questions per exam, since in that case all knowledge were identified at the same level.

Section 4.2 of this document describes methods and tools that could be used for the assessment of cybersecurity skills. Depending on the level of skills, different methods may be more suitable than others. In any case, the recommendation of the REWIRE project is for a practical approach to be applied (either through the use of specifically adapted questions – e.g. multiple choice questions that describe scenarios and aim at verifying knowledge based skills, or through the use of simulation environments and cyber ranges).

There are several key factors that play a role in designing an exercise. The first step is to identify the skills that are being evaluated and then establish difficulty or the level of the assessment.

The process of mapping skills to tasks is based on four main factors:

- the ordering of tasks should be such that it forms a coherent set of actions within an exercise. A chain of tasks has to maintain a natural flow. For example, requiring a candidate to connect to a server followed by scanning all open ports in a network does not make sense.
- the type of exercise being used for evaluation. Depending on the type of exercise, the tasks assigned vary. For example, to evaluate a candidate's skill in core network fundamentals, configuring a group of devices maybe a task in simulation type exercise whereas for the same skill simulating a man-in-the-middle attack can be used in a CTF type scenario.
- the level at which a skill is being evaluated. The higher this level is the more complex the corresponding task that has to be achieved. This has restrictions since certain skills cannot be more/less difficult than a certain threshold.
- The overall difficulty of the exercise. Difficult exercises can include more restrictions like tasks that are inter-dependent, or tasks that need to be solved in a specific order.

Taking all these in consideration, we derive the conclusion that higher level exercises can use a gamified approach rather than a simulation as the former is much more challenging. Also, the exercise type depends on the type of skills being evaluated, for knowledge-based skills a set of multiple-choice questions may suffice whereas for an attitude-based skill, (for example the ability to perform under high stress) a CTF based exercise maybe more appropriate.

On the subject of assessment of cybersecurity skills, this recommendation subscribes to the requirement for the practical assessment as depicted within the CONCORDIA Cybersecurity Skills Certification Framework, through the use of a suitable platform or tool.

The REWIRE project, will develop certification schemes for the assessment of knowledge and skills of four different Cybersecurity Roles of the ECSF (Deliverables R.4.6.1 – 3). The development of these schemes will be based on the CONCORDIA Cybersecurity Skills Certification Framework and this document. These certification schemes will be piloted as part of the project, and the assessment methods used per case shall be validated. This document will be further updated based on the validation results and the feedback of the interested parties.

6. List of Abbreviations and Acronyms

Abbreviation	Explanation/ Definition
ECSF	European Cybersecurity Skills Framework
CONCORDIA	Cyber security cOmpeteNCe fOr Research and InnovAtion (a European funded project)
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
NIST	National Institute of Standards and Technology
CEN/TC	European Committee for Standardization / Technical Committee
KSA	Knowledge, skills, and abilities
Cedefop	European Centre for the Development of Vocational Training
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISO	International Organization for Standardization
CISO	Chief Information Security Officer
e-cf	European e-Competence Framework
EQF	European qualifications framework
API	Application Programming Interface
DDoS	Distributed Denial-of-Service
PROCOM	The PROCOM framework - ICT Systems and Principles for Professionals - https://ocr.org.uk/Images/166244-centre-handbook.pdf
base64	is a group of binary-to-text encoding schemes that represent binary data (more specifically, a sequence of 8-bit bytes) in sequences of 24 bits that can be represented by four 6-bit Base64 digits.
Hex	Hexadecimal
CTF	Capture the flag

Table 7 List of abbreviations and acronyms

7. List of Figures

Figure 1. The analysis of the e-competencies of the CISO	10
Figure 2. EQF, e-cf and PROCOM levels	17
Figure 3. Sample Architectural Components of a Cyber Range.....	29

8. List of Tables

Table 1. Related Terms and Definitions	7
Table 2. Learning outcomes of Level 8 - EQF	12
Table 3. Learning outcomes of Level 7 - EQF	13
Table 4. Learning outcomes of Level 3 - EQF	14
Table 5. Learning outcomes of Level 6 - EQF	14
Table 6. Learning outcomes of Level 5 and 4 - EQF	15
Table 7 List of abbreviations and acronyms	31