June 2023

CyberSecurity for VET and SMEs

EUROPEAN FRAMEWORK ON CYBERSECURITY QUALIFICATIONS

DEVELOPED BY MINDSHIFT TALENT ADVISORY

WORK PACKAGE 2 - FRAMEWORK THROUGH COMPARISON
OF CURRENT NATIONAL COMPETENCIES ON CYBER SECURITY

TÜRKİYE ULUSAL AJANSI
TURKISH NATIONAL AGENCY

Funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. KA220-VET-C9588303

CONTENTS

About the project

SecureFuture – CyberSecurity for VET and SMEs – is an Erasmus+ project implemented between December 2022 and December 2024. The project is being conducted by a consortium of six partners from five counties, all partners with relevant expertise in vocational education and training (VET) and cybersecurity.

COUNTRY	ORGANISATION
Türkiye	Istanbul Ticaret Universitesi (coordinator)
Türkiye	Istanbul Valiligi
Portugal	Mindshift Talent Advisory
Spain	Media Creativa 2020
Italy	Pragma Engineering
Austria	Meta4 Innovations

The SecureFuture consortium identified that the current training provided at VET schools in the European Union (EU) does not live up to the needs of labour market or that there are countries without training on cybersecurity at this level. Besides, many short and medium-sized enterprises (SMEs) do not have qualified employees among their staff to protect their companies against cyber threats, and finding external assistance on cybersecurity is very costly.

Considering these aspects, the project is developing a European framework, curriculum and training content on cybersecurity to guide VET systems and SMEs who want to equip their students and employees with cybersecurity competences.

SYNOPSIS

The current European Framework on Cybersecurity Qualifications is the final output of the project's work package 2 (WP2) – Framework through comparison of current national competencies on cyber security.

The WP2 leader – Mindshift Talent Advisory – elaborated a workplan, guidelines and templates for all partners to implement a desk research on the state of the art in their countries regarding cybersecurity policies evolution in general, cybersecurity in VET provision and SMEs, their National Qualifications Frameworks (NQF) and current qualifications on cybersecurity. The conclusions reached on these topics are presented, as well as the competence areas and subjects suggested by parners to be included in the European Framework on Cybersecurity Qualifications.

Attached to this document, you can find the Summative EU report – which is available in English – with the comprehensive state of the art in each partner country regarding the previously mentioned topics on cybersecurity.

1. Framework

In this chapter, two tools used at European level in the development of qualifications are featured: the European Qualifications Framework (EQF) and the European Credit System for Vocational Education and Training (ECVET). Both approaches are introduced and applied to the European Framework on Cybersecurity Qualifications developed within the project.

1.1 NQF and EFQ level 4 comparative analysis

The European Qualifications Framework (EQF) is a common reference framework developed by the EU to facilitate the comparison and recognition of qualifications across different countries in Europe.The European Parliament and the Council recommendation, of May 22 2017, on the EQF for lifelong learning, states that:

> *Qualifications are more transparent and comparable when they are presented in documents that include a reference to the applicable EQF level and a description of the achieved learning outcomes.*
>
> *A wide range of stakeholders should be involved in implementing the EQF at European Union and national levels in order to ensure its broad support. Key stakeholders include all learners, education and training providers, qualifications authorities, quality assurance bodies, employers, trade unions, chambers of industry, commerce and skilled crafts, bodies involved in the recognition of academic and professional qualifications, employment services and services in charge of migrant integration.*
>
> *The EQF levels and learning outcomes' descriptors contribute to better transparency and comparability of qualifications of different national systems. They also contribute to a general shift towards a learning outcomes orientation in education and training.*

The design of the current European Framework in Cybersecurity Qualifications was planned following these principles, to facilitate, at national and European levels, the transfer and recognition of units of competence and further learning outcomes regarding a cybersecurity qualification.

The EQF level assigned to this new European Framework in Cybersecurity Qualifications is level 4, which is an intermediate level within the EQF, indicating a certain level of knowledge, skills, and responsability and autonomy. At this level, individuals are expected to possess a solid foundation of vocational or academic expertise, enabling them to perform various tasks independently or with limited supervision.

During the desk research phase, the SecureFuture consortium conducted a comparative analysis between the EQF level 4 and each corresponding National Qualification Framework (NQF) – all countries represented in the consortium have introduced national eight level frameworks. Next are presented the descriptors for EQF level 4 and the corresponding NQF level descriptors in each partner country.

EQF LEVEL 4 DESCRIPTORS' ELEMENTS		
Knowledge	**Skills**	**Responsibility and autonomy**
Described as theoretical and/or factual	Described as cognitive (involving the use of logical, intuitive and creative thinking) and practical (involving manual dexterity and the use of methods, materials, tools and instruments)	Described as the ability of the learner to apply knowledge and skills autonomously and with responsibility.

TÜRKİYE– NQF LEVEL 4		
Knowledge	**Skills**	**Responsibility and autonomy**
Have a moderate theoretical and operational knowledge and good factual knowledge in a field of work or study	Have cognitive and practical skills required to perform procedures and generate solutions to problems specific for a field of work or study	Take full responsibility in completing tasks within predictable, but changeable contexts Supervise the ordinary tasks of others, and take limited responsibility in evaluating and improving such tasks Meet own learning needs, and define proactive learning goals under guidance within the scope of lifelong learning approach Have awareness of the relationship between knowledge, skills, behaviours and attitudes in a field of work or study and social and moral issues and responsibilities

PORTUGAL – NQF LEVEL 4		
Knowledge	**Skills**	**Attitudes**

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

SPAIN – NQF LEVEL 4		
Knowledge	**Skills**	**Attitudes**
Theoretical and practical knowledge, depending on the professional, social and personal competences to be achieved.	A set of knowledge, skills and competence, the latter understood in terms of autonomy and responsibility, which responsibility, which make it possible to respond to the requirements of the productive sector, increase employability and favour social cohesion.	The Education Administrations, within the framework of their competences, shall promote the organisational and managerial pedagogical autonomy of the centres that provide vocational training, encourage teamwork among teachers and the development of training, research and innovation plans in their teaching field, as well as actions that favour the continuous improvement of training processes.

ITALY – NQF LEVEL 4		
Knowledge	**Skills**	**Competence**
Broad range of knowledge, integrated from a factual and/or conceptual dimension, deepened in some areas. Interpretive capacity.	Use also through adaptations, reformulations and rework a range of knowledge, methods practices and protocols, materials and tools, to solve problems, activating a set of cognitive relational, social and activation skills necessary to overcome increasing difficulties. Typically: problem solving, cooperation and multitasking	Ensuring the achievement of objectives, coordinating and integrating the activities and results also of others, participating in the process decision-making and implementation, in a normally predictable context, subject to unforeseen changes

AUSTRIA – NQF LEVEL 4		
Knowledge	**Skills**	**Competence**
He/she has:	In his/her field of work or study he/she is able to:	In his/her field of work or study he/she is able to:

an in-depth general education; theoretical knowledge in his/her field of work or study (*e.g.*, about facts and circumstances, principles, materials, processes, methods, connections, regulations and norms) to deal independently with common tasks and challenges, including with changing framework conditions; fundamental company-related business and legal knowledge; a university entrance qualification or knowledge needed to directly exercise a profession.	select common instruments, methods and procedures and use them appropriately; independently cope with standard tasks, including under changing conditions; analyse everyday problems considering theoretical knowledge, demonstrate different approaches to solutions and solve these problems independently; develop certain creative and networked thinking; take part in discussions in standard situations with familiar themes, present his/her own viewpoint and give reasons to substantiate this; independently research relevant information to fulfil his/her tasks from largely given sources, critically assess this and use it; present information in appropriate form (i.e., according to the situation and the target audience) and technically correct while using the correct language and using common communication techniques/technologies.	handle routine situations independently and behave appropriately according to the circumstances; work in a team and instruct/supervise others in common tasks.

1.2 ECVET implementation and allocation of ECVET points

The European Credit System for Vocational Education and Training (ECVET) was created by a Recommendation of the European Parliament and the European Council of 18 June 2009 with the aim of improving the recognition, accumulation and transfer of learning outcomes, supporting mobility and lifelong learning , as well as the creation of a system of EU credits in vocational education and training. This can be summarised in four main principles:

1. Units of learning outcomes
2. Accumulation and transfer of learning outcomes
3. Learning agreement and memorandum of understanding
4. ECVET (credit) points

Over the 10 years of its application, ECVET has contributed to the development of a better quality mobility experience through the use and documentation of learning outcomes units. However, the concept of ECVET points has not been generally applied and ECVET has not led to the development of a European credit system for vocational education and training. For this reason, next is provided the state of the art regarding the ECVET implementation and points allocation in each SecureFuture partner country. A 25-hour unit of competence is used as a reference to facilitate the understanding of the the assignment of ECVET points in each country.

TÜRKİYE: 25 hours = 1,25 ECVET point
Türkiye does not have a framework or guidelines for the attribution of ECVET points and credits for VET programmes but it explored the ECVET credit attribution via the general ECVET Recommendation: the attribution of 60 ECVET credits for each academic year. Considering this, the average ECVET point value for one technical course hour in Türkiye is 0,05 (25h = 1,25)

PORTUGAL: 25 hours = 1 ECVET point
In 2017, a national credit system for vocational education and training was created, aligned with ECVET principles and with the design of qualifications in terms of learning outcomes. Credit points are allocated to qualifications that integrate the National Qualification Catalogue. A full-time formal training year corresponds to 60 credit points, as proposed by the ECVET Recommendation, and credit points are distributed among the units that comprise the qualifications. Mostly, 25 hours correspond to 1 ECVET point.

SPAIN: 25 hours = 1 ECVET point

The Spanish VET system has implemented all ECVET principles except credit points. VET qualifications are expressed in learning outcomes and designed as learning units and modules. In a pilot experience, the general ECVET Recommendation was followed, with the attribution of 60 ECVET credits to each academic year. In average, 25 hours correspond to 1 ECVET point.

ITALY: 25 hours = 1,5 ECVET point

Since Italy does not have a credit system for vocational education, the attribution of ECVET points has been calculated by taking into consideration the three-year courses equivalent to 3000 hours. Considering this, the average ECVET value for one hour of training in Italy is 0,06, 25h corresponding to 1,5 ECVET points.

AUSTRIA: N/A

In 2013, a comprehensive national ECVET implementation strategy was presented aiming to employ the added value of ECVET to foster permeability and transparency within the national qualification system. Austria has been involved in aligning its vocational education and training systems with ECVET principles but predominantly only the learning agreements and memoranda of understanding were implemented.

Considering the heterogeneous use of ECVET in partner countries, the average ECVET points per hour of training, and aiming to achieve an easy and clear ECVET formula, the partnership of SecureFuture project agreed that in the European Framework in Cybersecurity Qualifications the ECVET points are allocated as follows:

1 hour of training = 0,05 ECVET points

20 hours of training = 1 ECVET point

As this new Cybersecurity Qualification includes 10 modules with a span of 120 hours, this means that:

1 module = 12 hours = 0,6 ECVET points

10 modules = 120 hours = 6 ECVET points

This way, the new Cybersecurity Qualification is developed taking into acount these parameters and corresponds to 6 ECVET points.

2. Background

The state of the art of cybersecurity in Türkiye, Portugal, Spain, Italy and Austria showcases a strong emphasis by government, SMEs and VET systems on addressing the evolving threats and challenges in the digital landscape in the last couple of decades. These countries have made significant progresses in developing cybersecurity frameworks, strategies and collaborations to protect critical assets, data and infrastructure, altough different levels of development were identified in each country. Detailed information on country developments can be found in the Summative EU report.

This chapter presents the main information collected by the project partners regarding the mapping of national qualifications in cybersecurity, as well as the suggestions of essential areas of competence to be included in the Framework.

2.1 Mapping of qualifications in cybersecurity

During the desk research phase, the project partners reviewed national frameworks in VET curricula and continuous training. The analysis of these country-specific frameworks aimed at finding key areas and trends to include in the SecureFuture Curriculum. A table summarising the reviewed frameworks is presented next.

	National qualifications		
Türkiye	Vocational and Technical Anatolian High School Cyber Security Programme VET curricula	Vocational Higher Cyber Security Programme VET curricula	Corporate Cybersecurity Training Certificate Programme Continuous training
Portugal	Technician/Specialist in Cybersecurity	Cybersecurity Manager	

	VET Curricula	Continuous training	
Spain	Networked Computer Systems Administration VET curricula	Advanced course in cybersecurity Continuous training	
Italy	Cybersecurity specialist VET curricula	Basic course in cybersecurity Continuous training	
Austria	Cybersecurity T-VET curricula	Risk manager on information security Continuous training	

As observed, all the partner countries have implemented VET courses and continuous training in cybersecurity. The reviewed VET curricula widelly differ in duration from one year (Türkiye) up to five years (Austria). Regarding continuous training, the analysed courses vary from 18 hours (Portugal) up to 100 hours (Türkiye). This array of courses and lenghts enriched the desk research and provide a strong basis for the definition of the competences to be featured in the European Framework on Cybersecurity Qualification.

Complete information about the qualifications mapped can be foun in the EU Summative Report.

2.2 Mapping of competences in cybersecurity

Along with the mapping of national qualifications on cybersecurity, the SecureFuture partners' desk research also allowed the elaboration of a comprehensive list of subjects in their cybersecurity national qualifications landscape. After being analysed, the subjects can be organised and summarised in the following list of main competence areas.

- Fundamentals of cybersecurity
- Programming and cryptography
- Cyber attacks
- Cybersecurity legislation, policies and standards
- Cybersecurity prevention & defence methods
- Intervention teams
- Cybersecurity management
- Software security
- Hardware security
- Network communication, security and management
- Mobile applications security
- Web applications security
- Internet of Things security
- Cloud computing security
- Database systems engineering, security and management
- Information infrastructures physical security
- End user security
- Cyber forensics

Besides this subjects adressed in the national qualifications, during the desk reasearch phase partners were also invited to provide their suggestions regarding the units of competence that should be included in the European Framework on Cybersecurity Qualifications considering EQF level 4. Each partner of SecureFuture project consulted national professionals related to cybersecurity to contribute to the current desk research, including for the referred suggestion of units of competence, which are listed next, without any specific ordering criteria.

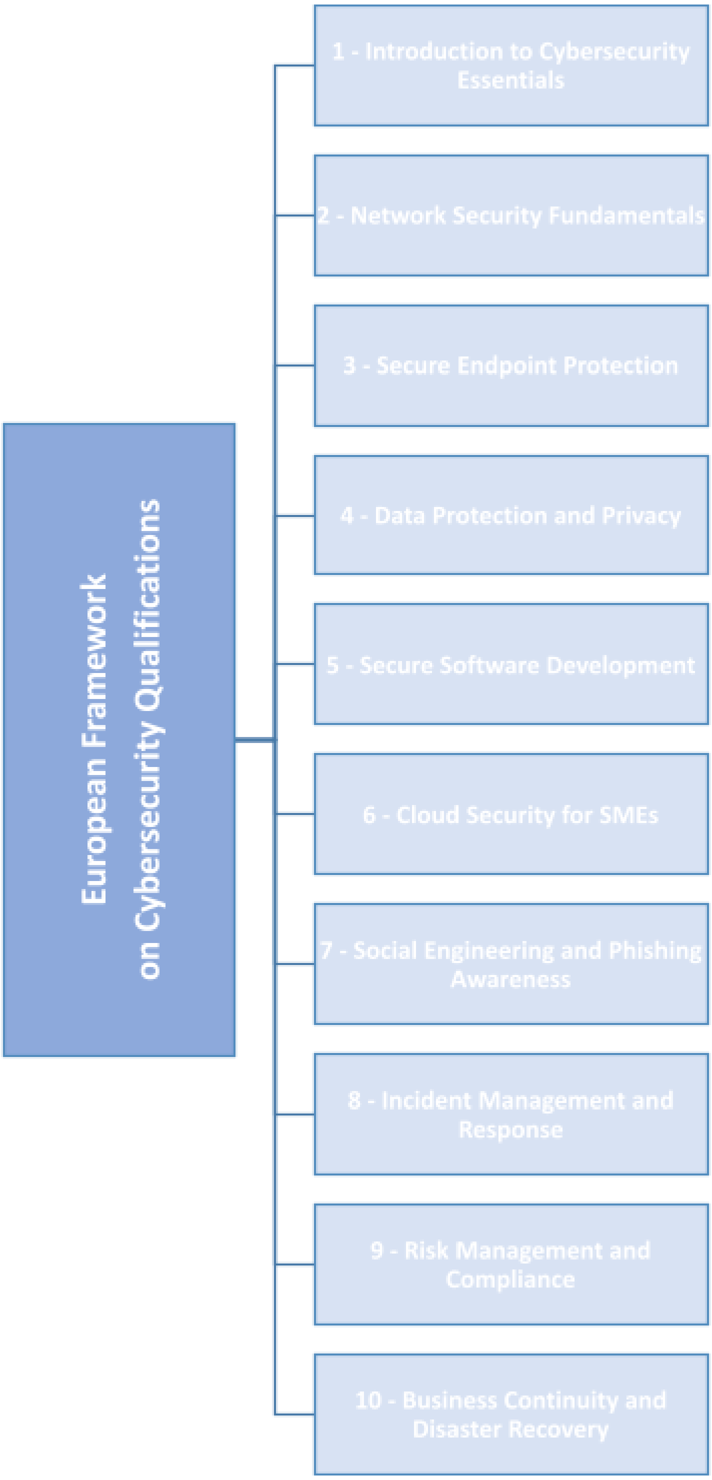
- Introduction and Historical Development of Cybersecurity
- Cybersecurity in Society and Social Media
- Cybersecurity in SMEs, Software and Hardware Security
- Desktop and Mobile Operation Systems
- IT Law, Digital Forensic and EU Regulations

- Cyberspace, Cyber Attacks and Prevention Methods
- Network, Data, Cloud Security and Risk Analysis in SMEs
- Network security
- Cybercrime
- Digital Forensics
- Information Security Management
- Cybersecurity law and ethics
- Cybersecurity Fundamentals for SMEs
- Secure Software Development
- Incident Response and Disaster Recovery
- Compliance and Regulatory Requirements
- Cyber Threat Intelligence
- Social Engineering Awareness
- Cloud Security
- Detection of attack: AI applied to Cybersecurity
- EU Data Protection Regulations
- E-learning Information Security
- Social Engineering Security Check - Identifying Hacker Attacks

Complete information about the competences mapped can be foun in the EU Summative Report.

3. Units of competence

Based on all the information collected by SecureFuture project partners during the desk research on the state of the art in their countries regarding cybersecurity, the ten suggested competence units for the European Framework on Cybersecurity Qualifications are presented below. These units embrace all areas and competences mentioned by the partnership as essential for the Framework.


European Framework on Cybersecurity Qualifications
1 - Introduction to Cybersecurity Essentials
2 - Network Security Fundamentals
3 - Secure Endpoint Protection
4 - Data Protection and Privacy
5 - Secure Software Development
6 - Cloud Security for SMEs
7 - Social Engineering and Phishing Awareness
8 - Incident Management and Response
9 - Risk Management and Compliance
10 - Business Continuity and Disaster Recovery

Next are presented subjects to be included in each of the units of competence. These subjects are some of the essential topics to be addressed in the ten units and do not limit the addition of other topics when defining their learning outcomes.

1

Introduction to Cybersecurity Essentials

- Overview of cybersecurity threats and risks for SMEs (e.g., concepts of cyber threat, cyber crime, cyber attack, hacking, identity theft, online fraud)
- Importance of cybersecurity for business operations
- Basic principles of cybersecurity (e.g., programming and cryptography)
- Security best practices for SMEs (prevention measures)

2 Network Security Fundamentals

- Understanding network architecture and components
- Securing network infrastructure
- Implementing firewalls and intrusion detection systems (defence technologies)
- Network monitoring and incident response

3 Secure Endpoint Protection

- Importance of endpoint security for SMEs
- Implementing antivirus and anti-malware solutions
- Securing mobile devices and remote access
- Endpoint security management and patching (e.g., AI applied to cybersecurity)

4 Data Protection and Privacy

- Data classification and handling sensitive information (e.g., concepts of privacy, intellectual property, cyber warfare)
- Introduction to data protection regulations (e.g., personal data, digital data, GDPR)
- Implementing data encryption and secure data storage
- Managing data breaches and incident response

5 Secure Software Development

- Understanding secure coding principles

- Common software vulnerabilities and mitigation techniques (e.g., input validation, buffer overflow)
- Secure software development life cycle (SDLC)
- Code review and testing for security

6
Cloud Security for SMEs

- Introduction to cloud computing and its security implications
- Securing cloud-based infrastructure and services
- Identity and access management in the cloud (including protection of personal data and digital identity)
- Data privacy and compliance in the cloud

7
Social Engineering and Phishing Awareness

- Understanding social engineering attacks and tactics
- Recognizing and avoiding phishing attempts (e.g., phishing scams, spear phishing, social media attacks)
- Employee awareness and training on social engineering
- Incident response and reporting procedures

8
Incident Management and Response

- Establishing an incident response plan
- Detecting, analysing, and containing security incidents (e.g., digital forensics, network logs)
- Incident response team roles and responsibilities
- Lessons learned and continuous improvement

9
Risk Management and Compliance

- Identifying and assessing cybersecurity risks for SMEs
- Establishing risk management frameworks
- Compliance with industry standards and regulations
- Incident reporting and compliance audits

10

Business Continuity and Disaster Recovery

- Understanding business continuity planning (governance)
- Developing disaster recovery strategies for SMEs
- Backing up and restoring critical data and systems
- Testing and maintaining business continuity plans

The ten suggested units of competence and subjects are the basis for the preparation of the Curriculum for the European Framework on Cybersecurity Qualifications EQF level 4.

4. Final remarks

The current European Framework on Cybersecurity Qualifications developed under the Erasmus+ project SecureFuture was throrughly drafted on the data provided by the project partners during the desk research phase on the state of the art of cybersecurirty in their countries. It takes into consideration the following parameters:

- compliance with EQF level 4, facilitating a standardised reference for a cybersecurity qualification and facilitating recognition across European borders
- assignment of 0,6 ECVET points to each unit of competence – the set of 10 units corresponding to 6 ECVET points
- suggestion of ten areas as units of competence and related contents.

All the defined requirements and foundations are to be considered in the development of the further European Cyber Security Curriculum, under projects' WP3, which, in turn, supports the development of WP4 – SecureFuture Training Content.

Together, the present Framework and the further Curriculum and Content are an innovative value proposition with strong potential to meet European countries' needs regarding training in cybersecurity for VET students and employees of SMEs – the main target groups of the project – and thus prepare well-trained cybersecurity professionals to defend European SMEs from cyber threats.

5. References

Compare national qualifications frameworks across Europe

https://europa.eu/europass/en/compare-qualifications

Description of the eight EQF levels

https://europa.eu/europass/en/description-eight-eqf-levels

European credit system for vocational education and training (ECVET)

www.cedefop.europa.eu/en/projects/european-credit-system-vocational-education-and-training-ecvet

Implementation of the European Qualifications Framework (EQF)

https://europa.eu/europass/en/implementation-european-qualifications-framework-eqf

National qualifications framework developments in Europe 2019

https://www.cedefop.europa.eu/files/8609_en.pdf

https://www.cedefop.europa.eu/files/4190_en.pdf