EUROPEAN UNION AGENCY
FOR CYBERSECURITY

USER MANUAL

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

SEPTEMBER 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use euskills@enisa.europa.eu.

ACKNOWLEDGEMENTS

This framework is the result of the expert opinion and agreement in the Ad-Hoc Working Group on the skills framework composed by Agata BEKIER, Vladlena BENSON, Jutta BREYER*, Fabio DI FRANCO, Sara GARCIA, Athanasios GRAMMATOPOULOS, Markku KORKIAKOSKI, Csaba KRASZNAY, Haralambos MOURATIDIS, Christina GEORGHIADOU, Erwin ORYE*, Edmundas PIESARSKAS, Nineta POLEMI*, Paresh RATHOD*, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN and Jan HAJNY.

Fabio DI FRANCO and Athanasios GRAMMATOPOULOS led this activity for ENISA.

LEGAL NOTICE

COPYRIGHT NOTICE

* Rapporteur of Ad-Hoc Working Group on the European Cybersecurity Skills Framework

ISBN: 978-92-9204-583-8 – DOI: 10.2824/95989

TABLE OF CONTENTS

1. INTRODUCTION 6

1.1 TARGET AUDIENCE 6

1.2 STRUCTURE OF THE MANUAL 6

2. UNDERSTANDING THE ECSF 8

2.1 THE ECSF DESIGN PRINCIPLES 10

2.1.1 Simple yet Comprehensive 10
2.1.2 Flexible and Scalable 10
2.1.3 Open and Impartial 10
2.1.4 European 11

2.2 THE MAIN BENEFITS PROVIDED BY THE ECSF 11

3. APPLICATIONS OF THE ECSF 14

3.1 EMPLOYING CYBERSECURITY PROFESSIONALS – APPLY THE ECSF AS AN ORGANISATION 16

3.2 SKILLING CYBERSECURITY PROFESSIONALS – APPLY THE ECSF AS A LEARNING PROVIDER 24

3.3 MAKING OWN CAREER CHOICES – APPLY THE ECSF AS AN INDIVIDUAL PROFESSIONAL 27

3.4 BUILDING CYBERSECURITY COMMUNITIES – APPLY THE ECSF AS A PROFESSIONAL ASSOCIATION 28

3.5 EMPOWERING THE SECTOR STRATEGICALLY – APPLY THE ECSF AS A POLICY MAKER 29

4. TERMS AND DEFINITIONS 30

5. REFERENCES 32

A ANNEX: CONNECTING THE ECSF TO OTHER EU STANDARDS AND FRAMEWORKS 34

A.1 EN16234-1 E-CF A COMMON EUROPEAN REFERENCE FRAMEWORK FOR ICT PROFESSIONALS IN ALL SECTORS 34

A.2 EUROPEAN ICT PROFESSIONAL ROLE PROFILES 35

A.3 EUROPEAN QUALIFICATIONS FRAMEWORK 36

A.4 ESCO - EUROPEAN CLASSIFICATION OF SKILLS, COMPETENCES AND OCCUPATIONS 36

B ANNEX: USE CASES 38

B.1 USE CASE FROM CONCORDIA H2020 PROJECT 38

B.2 USE CASE FROM SPARTA H2020 PROJECT 40

B.3 USE CASE FROM INCIBE 42

B.4 USE CASE FROM THE EUROPEAN CYBER SECURITY ORGANISATION (ECSO) 44

B.5 USE CASE FROM ISC2 46

B.6 USE CASE FROM ISACA 47

B.7 USE CASE FROM SANS/GIAC 50

EXECUTIVE SUMMARY

The cybersecurity workforce shortage and skills gap is a major concern for both economic development and national security. By looking into the problem, ENISA identified Europe's need for a comprehensive approach to define a set of cybersecurity roles and skills that could be leveraged to reduce the shortage and the skills gap. ENISA has worked on the development of such a framework and presents the **European Cybersecurity Skills Framework (ECSF)**, which is intended to strengthen European cybersecurity culture by providing a common European language across communities, taking an essential step forward towards Europe's digital future.

The European Cybersecurity Skills Framework (ECSF) is intended to strengthen European cybersecurity culture by providing a common European language across communities, taking an essential step forward towards Europe's digital future.

The ECSF provides a practical tool to **support the identification and articulation of tasks, competences, skills and knowledge associated with** the roles of European **cybersecurity professionals**. The main purpose of the framework is to **create a common understanding** between individuals, employers and providers of learning programmes across EU Member States, making it a valuable tool to bridge the gap between the cybersecurity professional workplace and learning environments.

The framework describes the most important requirements of a professional cybersecurity workplace by defining a **set of 12 typical cybersecurity professional role profiles**. These profiles provide a common understanding of the main cybersecurity missions, tasks and skills needed in a professional cybersecurity context, making it the perfect reference for profiling skills and knowledge needed by cybersecurity professionals. The framework was designed to be easily understood and comprehensive enough to provide appropriate in-depth cybersecurity insights as well as flexible enough to allow customisation based on each user's needs. By incorporating all stakeholder perspectives, the framework is applicable to all types of organisations and supports the development of all cybersecurity professions.

The ECSF is the result of work conducted by ENISA's Ad-Hoc Working Group on the European Cybersecurity Skills Framework[1] formed by experts representing various views. The developed framework is based on an analysis of existing frameworks, the results and findings from research on market needs and agreement among experts. User case studies and indicative examples, inspired by various workplace and learning environments, demonstrate the practical implementation of this framework and support this work.

The main benefits of using the ECSF were found to be:

- ensuring a **common terminology** and **shared understanding** regarding cybersecurity professionals across the EU;
- identifying the **critical skills-set** required from the perspective of the cybersecurity workforce to support its further development and enhancement;
- promoting **harmonisation** in cybersecurity **education**, **training** and **workforce development** programmes.

This ECSF User Manual provides a comprehensive overview of the ECSF's main scope, framework principles and application opportunities. The primary purpose of the manual is to make the ECSF easily accessible by, understandable for, and usable by all stakeholders with an active role or a need for appropriately skilled cybersecurity professionals.

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

1. INTRODUCTION

The shortage of cybersecurity skills is one of the key challenges that needs to be addressed for a cyber secure European Union. More specifically, there is a lack of skilled and qualified personnel in the labour market to take on roles in cybersecurity and who can sufficiently address the evolving cyber threats and the emerging cybersecurity challenges. The gap in cybersecurity skills has a number of underlying drivers. These include an insufficient level of understanding of the competences and skills needed in the cybersecurity discipline between different actors in the market for cybersecurity skills. Over the years, this has become a well-documented problem[2], which continues to significantly affect countries at European and international level.

In order to reduce the current and the future skills gap and shortage, more cybersecurity professionals with appropriate skill sets are needed. To this end, the European Skills Agenda[3], the Digital Education Action Plan[4], and the Pact for Skills[5] remain important vehicles for mobilising stakeholders to work together towards the goals of the Digital Decade[6] by creating more and better opportunities for training.

In this context, ENISA launched an Ad Hoc Working Group on the European Cybersecurity Skills Framework[7] in December 2020. A multi-disciplinary group of experts was brought together with the aim of promoting harmonisation of cybersecurity education, training and workforce development concepts. The developed framework (ECSF) provides an open European tool to build a common understanding of the cybersecurity professional role profiles and common mappings with the appropriate skills and competences required. This work provides the basis for joining forces in a capacity building programme for the European cybersecurity workforce in accordance with ongoing market demand.

The ECSF provides an open European tool to build a common understanding of the cybersecurity professional role profiles and common mappings with the appropriate skills and competences required.

1.1 TARGET AUDIENCE

Whilst the ultimate scope of the content of the ECSF framework is cybersecurity core professionals, a particular emphasis is also placed on the ECSF target groups of non-cybersecurity experts who need a comprehensive view of the discipline. This focus makes the framework easy to understand for all stakeholders concerned.

The target audience for the ECSF is organisations' leadership teams, human resources (HR) and cybersecurity functions, cybersecurity professionals, newcomers and cyber enthusiasts, as well as providers of learning programmes of all types in the public and private context, sector associations, market researchers, and policy makers.

The ultimate scope of the ECSF framework is cybersecurity core professionals, while emphasis is also placed on non-cybersecurity experts who need a comprehensive view of the discipline.

1.2 STRUCTURE OF THE MANUAL

The user manual is structured as follows:

- Chapter 1 introduces the key challenges that highlight the need to create a framework for cybersecurity skills as well as the target audience for this work;
- Chapter 2 presents the ECSF design principles as well as the key benefits for using it;

[2] ENISA, 2020, Cybersecurity Skills Development in the EU https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1196
[4] https://education.ec.europa.eu/focus-topics/digital-education/action-plan
[5] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197
[6] https://digital-strategy.ec.europa.eu/en/node/157
[7] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

- Chapter 3 explains the different applications of the ECSF from various viewpoints.

Additionally, the document includes two (2) Annexes that support the ECSF user manual and its objectives:

- Annex A connects the ECSF to other EU standards and frameworks.
  The objective of this Annex is to connect the ECSF with existing recognised European standards and frameworks that are relevant to this work.
- Annex B lists Use Cases of the ECSF.
  The objective of this Annex is to provide real case scenarios to showcase the practical implementation of this framework.

2. UNDERSTANDING THE ECSF

The ECSF is comprised of a representative set of **12 role profiles for cybersecurity professionals** (presented in Figure 1) that are typically required and applied within organisations deploying cybersecurity professionals. Each profile is defined by a common template that incorporates key set criteria (i.e. title, alternative titles, summary statement, mission, main tasks, key skills, key knowledge, e-Competences). The content of each criterion is tailored to each role but is subject to possible adaption to enable flexible implementation to meet specific situations and requirements.

Figure 1: The ECSF's 12 Role Profiles for Cybersecurity Professionals

The ECSF introduces a representative set of 12 role profiles for cybersecurity professionals (typically required and applied within organisations) in an EU-agreed, practice-driven format dedicated to the cybersecurity professional domain.

The 12 role profiles for cybersecurity professionals are provided in an EU-agreed, practice-driven format dedicated to the cybersecurity professional domain. The profiles are easily understood and offer alternative entry points according to context, perspective and need. Through these profiles, the ECSF can be used as a common reference and communication tool that can be applied across different organisations and countries for a common mutual internal and external understanding.

The structure of each role profile is outlined in Table 1 below.

Table 1: The components of each ECSF role profile

Profile title	The name of the Professional Role Profile
Alternative title(s)	Lists typical alternative titles under the same profile.
Summary statement	Indicates the main purpose of the profile.
Mission	Describes the rationale of the profile.
Deliverable(s)	A list of typical outcomes of the profile, also explaining profile relevance from a non-expert viewpoint.
Main task(s)	A list of typical tasks performed by the profiled role.
Key skill(s)	A list of abilities needed to perform the work functions and duties of the role. Soft skills and ethics are made explicit in some cases.
Key knowledge	A list of the essential knowledge required to perform the work functions and duties in the profiled role.
e-Competences (EN16234-1 e-CF)	Connection to EN16234-1 e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors.

As presented on Table 1, the profile for each role is populated by a set of descriptive items designed to provide a snapshot of the role in terms of its description, tasks and competences. Titles and typical alternative titles can be used as a quick reference to guide ECSF users to the most appropriate role profiles for their application.

Components of the role profiles **can be altered** to better cover the stakeholder's needs, and **role profiles** (from the ECSF and other frameworks) **can be mixed together** for the same reason. More information on applying the ECSF is given on Chapter 3.

Soft skills (also called transversal, transferrable or behavioural skills) are components that are necessary in any professional skill set; thus, such skills are also needed for professionals in the cybersecurity domain. A wide range of skills fall under soft skills such as the abilities to communicate, collaborate with others, report, influence, think critically, and manage time and stress. Key soft skills are incorporated in the key skills component.

For instance, the role profile for a Chief Information Security Officer (CISO) includes as key skills the abilities to influence, lead, communicate, cooperate and collaborate. All of these are essential skills if a CISO is to achieve her or his missions and tasks. Based on a stakeholder's needs, more soft skills might be added to the profile for a CISO or a mapping with a soft skill framework may be done.

Ethics is also an important cross-cutting element that impacts all the aspects of cybersecurity and is therefore an essential skill component within the European Cybersecurity Skills Framework (ECSF). In the context of cybersecurity, ethics is about what decisions are aligned with our values and what is morally acceptable for both the data owner and the organisation. As cybersecurity professionals could gain privileged access to various types of information, even sensitive information, ethical awareness is an important value they should have. Apart from that, ethical decision-making is an important skill that cybersecurity professionals should have as

their decisions affect other individuals. As in the case of soft skills, the ECSF explicitly analysed whether the ethical side of the sector is aligned with European values and ethics.

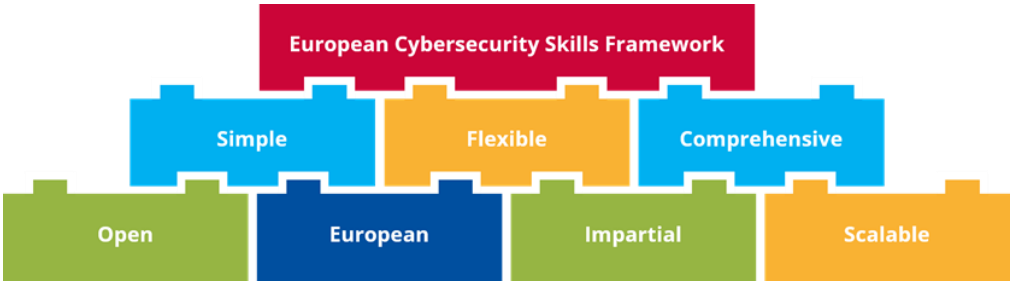
A more detailed analysis of the soft and ethical skills might be done by the interested party since the framework is flexible and adaptable.

2.1 THE ECSF DESIGN PRINCIPLES

The European Cybersecurity Skills Framework is based on a number of principles designed to cover stakeholder needs. This offers easy understanding, adoption and application of the framework whilst maintaining relevance and impact in the short and longer-term.

The ECSF is based on principles designed to cover stakeholder needs, offering easy understanding, adoption and application whilst maintaining relevance and impact in the short and longer-term.

Figure 2: The ECSF's design principles



2.1.1 Simple yet Comprehensive

The framework is designed to be suitably general to ensure that it may be easily understood and applied by a wider audience. At the same time, it includes sufficient detail to provide in-depth cybersecurity insights. These attributes facilitate use of the framework across a broad spectrum of activities and environments and by stakeholders from a variety of backgrounds (e.g. organisations of different sizes, technical expertise of varying intensity and business sectors with different core activities).

This has been achieved by applying the appropriate level of detail to the content of the ECSF that is not too specific nor too abstract. Offering 12 profiles, the ECSF covers a broad spectrum of diverse work activities but maintains an easy-to-use format.

2.1.2 Flexible and Scalable

By adopting a modular approach and a flexible structure the framework enables each component to be extendable or used independently. These characteristics support further extension of the ECSF and/or linkage to other frameworks to expand its applications.

Applying this flexibility, the profiles and their components, as defined by the ECSF, can be applied on a module-by-module basis allowing each to be adapted to meet specific needs. This flexibility ensures the relevance of the framework over the years and will also allow simple updates to the framework in the future.

2.1.3 Open and Impartial

The framework has been developed with input from a large and diverse working group of professional cybersecurity experts. In order to develop an impartial framework, ENISA established this group from a variety of experts from various backgrounds. By involving experts with different backgrounds, the development process of the framework followed a multi-perspective approach eliminating any bias towards specific areas of interest. Furthermore, as an ENISA publication, the framework is publicly available, accessible and open.

The ECSF profiles and components have been developed based upon a multi-stakeholder perspective with a focus not only upon the viewpoint of employment in cybersecurity but also from the perspective of providers of learning programmes. Furthermore, the veracity of the framework has been enhanced by engagement and reviews from a variety of additional stakeholders.

2.1.4 European

Driven by the requirement to minimise gaps in cybersecurity skills and shortages in the workforce across Europe, the ECSF needed to be compliant with specific European requirements, to enable easy adoption and use by European organisations. This direction was informed by complying with existing European standards and frameworks.

The ECSF connects well with the current European ICT professional landscape to ensure easy take-up and broad recognition. The ECSF takes the best benefit from existing experiences and structures and provides consistent links with relevant EU ICT professional standards and frameworks. The profiles defined by the framework are designed to be compliant and complementary to European laws and regulations and to enhance approaches to European ethics as identified in the European marketplace. The ECSF takes into consideration the requirements for the protection of data and privacy set by European regulations, common job roles requested by the European market, and European standards and frameworks used in the ICT sector.

2.2 THE MAIN BENEFITS PROVIDED BY THE ECSF

The ECSF is an easy to use yet comprehensive tool. It is based upon recent market studies, the collaboration of cybersecurity experts and an analysis of the broader cybersecurity and ICT frameworks landscape. It thus expresses the relevant needs of the European market. It is comprised of 12 typical professional roles in cybersecurity, with a related summary statement, mission, observable outcomes (deliverables), tasks, competences, skills, knowledge and proficiency levels, as required and applied in the context of work in Europe, to be understood and used across Europe.

The ECSF provides an unambiguous reference to identify and reduce current and future cybersecurity skills shortages and gaps. It is generic but at the same time sufficiently granular to give the EU market a clear taxonomy of skills, competences and occupations in the cybersecurity workforce. Furthermore, it may be easily connected with other existing structures and frameworks in associated fields.

The ECSF provides an unambiguous reference to identify and reduce current and future cybersecurity skills shortages and gaps.

Using the ECSF as a common European language for professional cybersecurity roles, skills, knowledge, and competences offers many benefits some of which are listed below.

1. Using the ECSF ensures a common terminology and shared understanding between cybersecurity professional demand (workplace, recruitment) and supply (qualification, training, assessment and recognition) across the EU.
2. The ECSF supports the identification of critical skill set requirements from the perspective of the workforce. It enables providers of learning programmes to support the development of critical skills and policy makers to support targeted initiatives to mitigate identified gaps in skills.
3. The ECSF helps in understanding professional cybersecurity roles and the required essential skills, and relevant legislation. In particular, non-experts and HR departments are able to better understand requirements for cybersecurity resource planning, recruitment and career planning.
4. The ECSF promotes harmonisation in cybersecurity education, training, and workforce development. Additionally, the use of a common European language in cybersecurity skills and roles relates directly to the entire ICT professional domain.

5. The ECSF contributes to achieving better resilience to cyber-attacks and to ensuring secure ICT systems across society. It provides a standard structure and gives advice on how to enforce capacity building in the European cybersecurity workforce.

The ECSF provides additional benefits based on the type of stakeholder. An example of the main stakeholders and key associated main benefits is shown in 3.

Figure 3: An example of the main ECSF beneficiaries expressing the need of a common Risk Manager definition

A detailed list of potential applications and benefits in using the ECSF based on stakeholders is shown in Table 2.

Table 2: The ECSF potential applications and benefits for stakeholders

Stakeholder	Benefits of using the ECSF

Organisations	• supports the development of a cybersecurity strategy and organisation structure
	• supports the development of cybersecurity human resource planning
	• provides support in the recruitment process, in particular:
	  ○ the identification of cybersecurity role requirements
	  ○ the assessment of cybersecurity candidates
	• provides analysis of cybersecurity role and skills gap and consequent forecasting of needs at individual, team or organisational level
	• defines development and training plans at individual, team or organisational level
	• supports the evaluation of cybersecurity roles by helping in building customised templates for cybersecurity roles
	• provides a common and easily understood language for cybersecurity tenders, procurement, vacancies and audits

Providers of learning programmes	• supports the design of learning programmes and curricula, re-design and maintenance • offers collaboration across institutions and mobility in learning programmes, e.g. cross-European learning programmes from multiple institutions • promotes offerings of learning programmes and raises awareness • positions learning outcomes in a real workplace context • supports assessment and recognition processes • provides career orientation to students

Individuals	• supports individuals in making professional career choices and positioning themselves • widens learning perspectives, opens new career paths and promotes professional development to support reskilling and upskilling • helps understand practical workplace requirements and job expectations in more detail • identifies formal and non-formal learning paths • provides support in building career paths
Professional associations	• allows the consolidation of stakeholder communities to support knowledge sharing, new developments, improvements, and further implementation in EU member states • provides support in conducting market analysis and presenting the results in a shared language • helps provide comprehensive professional guidance in the cybersecurity sector
Policy makers and government stakeholders	• supports a common understanding in the cybersecurity field • stimulates priority planning and cybersecurity capacity building • allows a mapping of many cybersecurity initiatives based on the ECSF profiles • supports policy initiatives based on the data analysis
All	• offers a common language for all stakeholders • accelerates collaboration by providing a common reference starting point • provides a shared reference to gather and present cybersecurity professional related information and needs at all levels, at national, European and international levels

3. APPLICATIONS OF THE ECSF

This chapter demonstrates how the European Cybersecurity Skills Framework (ECSF) can be applied in a modular and flexible way based on the needs of different stakeholders.

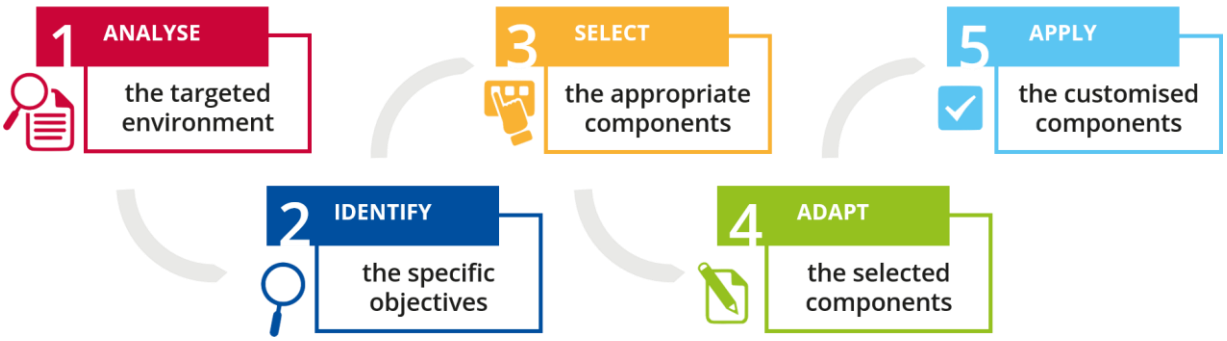
Specific use and practical application depend on many factors such as the market perspective, organisation size, the context of a particular performance and overall purpose.

The 12 role profiles for cybersecurity professionals defined by the ECSF are a flexible tool and a standard European reference for customised use in a particular context.

The following general five-step guide provides basic orientation:

The 12 role profiles defined by the ECSF are a flexible tool and a standard European reference for customised use in a particular context.

Figure 4: A modular five-step guide to apply the ECSF



1. **Analyse** the situation of the target environment.
   Collect and process the appropriate information needed about the cybersecurity related condition of the target environment (e.g. an organisation) to create a baseline. Identify the parties involved and the goal to be achieved.

2. **Identify** specific objectives to be achieved.
   Look into the status of the target environment and identify any specific cybersecurity-related requirements to be covered or any objective to be achieved by the targeted environment. Depending on the situation, it may be possible to use the ECSF as a taxonomy to identify the objectives in question.

3. **Select** the appropriate components of the ECSF.
   Review the ECSF profiles and select profiles that are relevant to a particular situation. Then select the components that assist in covering the needs or achieving the required objectives of the targeted environment.

4. **Adapt** the selected components according to your needs.
   Make appropriate changes on selected components to better fit a particular situation and/or targeted environment. The ECSF profiles and/or their components can be

mixed, split, or brought into a sector specific context according to the needs of each situation.

5. **Apply** the customised components to the target environment.
   Take action using the tailored ECSF components to cover security related objectives required to improve the situation of the target environment and to achieve the organisational goal.

Table 3 presents some indicative examples of the ECSF applications following the five steps presented above.

Table 3: The ECSF modular approach in practice

Example	Step	Description
Employing cybersecurity professionals in an organisation	1. Analyse	Analyse the current cybersecurity-related state of the organisation.
	2. Identify	Identify the lack of personnel to handle the increase in cybersecurity issues.
	3. Select	Select the appropriate task from an ECSF profile that articulates an identified shortage of or gap in specific skills.
	4. Adapt	Combine the ECSF profiles with tasks of interest to the organisation and structure new roles with the updated tasks, skills and knowledge to meet the changing organisational needs and create amended cybersecurity roles.
	5. Apply	Use the newly-generated profile to create job vacancies targeted on the specific needs of the organisation.
Skilling cybersecurity professionals	1. Analyse	Understand the business objectives and strategy of the organisation.
	2. Identify	Identify any lack of expertise and personnel in cybersecurity related areas.
	3. Select	Use the ECSF profile(s) to identify the associated skills and knowledge that the organisation lacks.
	4. Adapt	Analyse selected skills and knowledge from the ECSF to identify the training needs of a cybersecurity professional to meet the organisation's needs.
	5. Apply	Identify training interventions to enhance the competence of the organisation's workforce.
Making own career choices	1. Analyse	Choose a career path you are interested.
	2. Identify	Identify your lack of skills and the knowledge required to move into the cybersecurity sector.
	3. Select	Identify the ECSF profile(s) that you find useful from the perspective of career development, and use the connected skills, knowledge and competences as guidelines for reskilling and upskilling.

	4. Adapt	Enhance the selected ECSF profiles by including additional skills and knowledge based on individual needs.
	5. Apply	Identify a training programme incorporating the majority of the skills and knowledge development required to reskill or upskill for the profile.

3.1 EMPLOYING CYBERSECURITY PROFESSIONALS – APPLY THE ECSF AS AN ORGANISATION

The ECSF provides a standard reference set of 12 typical roles executed by cybersecurity professionals from an organisational perspective, covering the cybersecurity needs of the organisations and the cybersecurity processes that need to be followed in order to secure their business, products, services and their supply chains. **The framework thus provides a valuable guide and roadmap not only for building, expanding and running cybersecurity related functions within an organisation but also for ensuring its cybersecurity related mission, vision and goals are met.** Thus, an organisation can use the ECSF as a starting point or guide to quickly and easily access the primary roles needed to manage their cybersecurity risks and build up their cybersecurity approach. At the same time, the ECSF profiles provide a common understanding among the parties involved regarding an organisation's cybersecurity roles.

The ECSF can be used as guide and roadmap providing a common understanding among the parties involved regarding an organisation's cybersecurity roles.

Three indicative examples, which are presented later in this chapter, aim to showcase the practical implementation of the framework in the:

I. enhancement of the cybersecurity practices of a small company;
II. recruitment process of a large company with increasing compliance requirements;
III. planning of cybersecurity resources in a large organisation.

Example I: *Enhancing the cybersecurity practices of a small company* presents the application of the ECSF to address the needs of a small company seeking to enhance its cybersecurity structure and practise. It shows how a company might use the ECSF to support the development of a cybersecurity strategy, including the planning of human resources for cybersecurity and planning the procurement of cybersecurity.

By using the ECSF as a starting point or as a guide, the company does not need to invent or research basic roles needed to improve its cybersecurity posture. The roles can be granted to different persons or can be merged to be undertaken by just one or only a few persons depending upon the strategy, requirements, needs and budget.

The example also shows how the ECSF can support the organisation in the recruitment process by identifying the cybersecurity roles and responsibilities that are needed inside a small company. In this example, a cybersecurity role and skills gap analysis and consequent forecasting of needs at the organisational level are also provided. Apart from supporting the human resource processes in recruitment, the ECSF also provides a common language for procuring cybersecurity services.

Example I: Enhancing the cybersecurity practices of a small company

A small cloud services company became successful in just a few months after the founders, siblings Alicia and Max, implemented their idea for an innovative solution. Alicia was the expert 'techie' genius while Max was a marketing genius. Unfortunately, neither of them had any experience in running or building a company. After a year the company started to take off and so they moved into their own office and employed staff to grow the business. During this

expansion phase, no one considered organising the company. Many roles and duties were shared, and challenges were handled in an ad-hoc way. Fortunately, no serious cybersecurity incident occurred during this transition phase.

Eventually, the company gained some media exposure which went viral resulting in increased interest by new investors and clients towards the small start-up. However, larger clients and investors demanded assurance and proof of adequate security measures and an organisation structure before getting involved with the company. The founders realised that they would have to really shape things up inside their organisation. They were aware that the key to **the success of the organisation** was the employees and, to enable the organisation to flourish and offer resilient services, **it was essential to define their cybersecurity roles and responsibilities**. However, the question to be answered was what organisation setup was needed and which roles and what kind of competences did the organisation need?

Funders **used the ECSF and identified that their organisation required five key roles** to support their cybersecurity baseline:

- a strategic cybersecurity manager (CISO)
- a cybersecurity legal officer
- a cybersecurity architect
- a few cybersecurity implementers
- a cyber incident responder.

Looking internally to **identify** whether their **employees** were **able to cover these roles**, they found that their legal officer was already managing compliance with legal and regulatory frameworks and that she had an interest in **enriching** her **competences in privacy and cybersecurity** legal matters. Human Resources would be able **to support upskilling by using** a list of key **knowledge** and **skills** obtained **from the ECSF**.

The ICT Architect of the organisation had prior experience in secure networks design and therefore with additional **training to update and enrich** her **competence** he could also **cover the organisation's architectural cybersecurity requirements**.

The system administrators were following many cybersecurity best practices but worked mostly in an ad-hoc way without a strategy or structure. Consequently, the founders **identified a need to recruit a Strategic Cybersecurity Manager**. The Recruitment Officer was tasked with **drafting a job description based on the ECSF's CISO profile** and with listing the vacancy on their website.

Finally, it was established that the company's incident response functions needed to operate 24/7 to assure the continuous operation of services.

Figure 5: The key roles needed as identified using the ECSF and the actions to be taken

Example I showcased how useful the ECSF can be for the following benefits:

- understanding cybersecurity roles
- identifying workforce requirements
- evaluating processes and structure
- reskilling and/or upskilling employees
- supporting the recruitment process
- building cybersecurity capacity
- building a cybersecure and trusted organisation
- building resilience against cyberattacks.

Figure 6: Benefits of using the ECSF as shown by Example I

***Example II**: Crafting a job description* demonstrates the application of the ECSF when creating a job description. It shows how ECSF can be beneficial from the perspective of human resources without the need to have a deep understanding of the cybersecurity profession. This example shows how a job vacancy may be created and how to avoid the creation of misleading or confusing expectations and how to attract appropriately skilled personnel. It also demonstrates how to combine the components of an ECSF role profile and how to adapt them according to the job needs of an organisation.

This example demonstrates how an organisation can use the ECSF to create a description of a role. Even without an HR background, it is possible to define the tasks, skills and knowledge required of a candidate for recruitment by knowing the mission of the role. Apart from providing support to the recruitment process, the ECSF can also help the company to define training plans for newly recruited personnel. It is noteworthy that the ECSF not only provides a common language for cybersecurity procurement but also for audit purposes, especially where the principle of accountability is being implemented, and an essential and clear segregation of duties is required.

Example II: Crafting a job description

A large insurance company is extending its portfolio into cybersecurity insurance as many customers are seeking this service. After a slight internal restructuring and the updating of the personnel inventory, the company decides to add cybersecurity to the compliance department. Consequently, the compliance department management concludes that **they need to recruit a Cyber Compliance Officer** to support the new mission.

The company's HR department is tasked with **finding and recruiting the most suitable candidate**. As cybersecurity is a new area for the organisation, HR must also **create a role description**. To define this new role, **HR interviews** knowledgeable **managers and staff** to **identify** the **needs** and the **key tasks** for this position. These needs are identified and the key tasks selected are as follows:

- ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations;
- identify and document gaps in compliance;
- develop an audit plan describing the frameworks, standards, procedures and auditing tests;
- execute the audit plan and collect evidence and measurements;
- develop and communicate audit results (reporting).

The responsible HR officer recognises that this is a complex role and that no recruitment templates to fit this role are available. Therefore, **a new role description and template must be created** and approved by management.

The HR officer, now **using the ECSF, analyses different roles within the framework**. The specified duties are included in **the key tasks identified in the roles** of **Cyber Legal, Policy & Compliance Officer** and **Cybersecurity Auditor**.

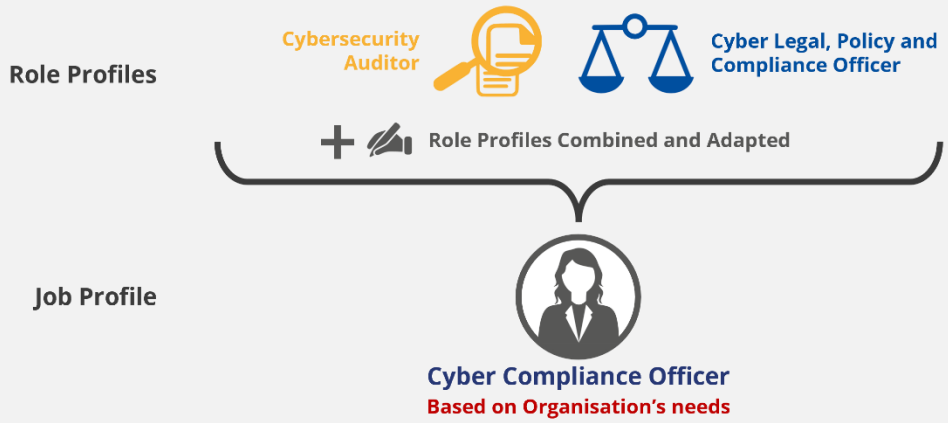
To perform these tasks, the identified **skills and the knowledge required** are as follows:

- Skills
  - understand the implications of modifications of the legal framework to the organisation's cybersecurity and data protection strategy and policies;
  - follow and practice auditing frameworks, standards and methodologies;
  - apply auditing tools and techniques;
  - work as part of a team and collaborate with colleagues.
- Knowledge
  - advanced knowledge of National, EU and international cybersecurity and related privacy standards, legislation, policies and regulations;
  - knowledge of information security compliance and regulatory requirements at the international, national and EU level;

- basic understanding of data storage, processing and protections within systems, services and infrastructures.

A **new role description** tailored to the companies needs may now be created by **mapping and combining** parts of the profile for the role of **Cyber Legal, Policy & Compliance Officer** and parts of the profile for the role of **Cybersecurity Auditor**. Significantly, by mapping to the framework, this new unique role is **based upon the core content of the ECSF**. This provides a uniform and structured role that may be traced back to its origin.

Figure 7: Cybersecurity job profile created based on the ECSF role profiles



Following this mapping to the ECSF, the role description required is available and can be used to draft the role and subsequent job description that HR needs to obtain internal approval and publish on the company's recruitment website. Further elements, such as profile mission, may be used as the introductory text for the publication of this vacancy.

Example II demonstrated how useful the ECSF can be for the following benefits:

- understanding cybersecurity roles
- identifying workforce requirements
- identifying role requirements
- supporting the recruitment process
- supporting the building of a customised vacancy template
- using a common language for vacancies.

Figure 8: Benefits of using the ECSF presented by Example II

***Example III**: A large corporation with its main business outside ICT needs to setup a cybersecurity department* demonstrates the application of the ECSF when creating a new cybersecurity department and preparing a cybersecurity strategy for the corporation. It also proposes a categorisation of the 12 profiles into four (4) macro areas for high-level understanding and communication. It shows how a large organisation might use the ECSF to support the development of a cybersecurity strategy, including human resource planning and talent development in cybersecurity.

Example III: A large corporation with its main business outside ICT needs to setup a cybersecurity department

A large corporation with a core business not related to ICT or cybersecurity services realised the need to protect its valuable assets from cybersecurity threats. In fact, the adopted business strategy incorporated a massive plan for the digitisation of business processes and the dependency on ICT was becoming significantly higher for critical business operations.

As the company did not have any internal expertise to handle cybersecurity risks, the board decided to hire a Chief Security Information Officer (CISO) to **define the overall cybersecurity** strategy in alignment with the company business objectives. This would also require **setting up a department** for **dealing with cybersecurity risks**.

The CISO, freshly appointed, **used the ECSF as a guideline** and **as a** solid **reference** for the **cybersecurity roles needed** to handle its cybersecurity risks. She used it as a **flexible tool** to help **structure a cybersecurity department**. She also recognised that, to provide a clear schematic, it would be useful to place **the ECSF roles in the context of a management circle**, under four (4) macro areas: a) Plan, b) Implement, c) Operate and d) Improve.

Figure 9: Placing the ECSF role profiles in the context of a management circle

In the Plan macro area, priorities and targets were set, strategies, policies and action plans developed, architectures defined, resources allocated. In this macro area, the CISO, the Policy and Compliance Officer, the Risk Manager and the Architect profiles were positioned naturally.

Implementation of cybersecurity measures (Implementer) and training and awareness raising (Educator) were allocated to the Implement macro area.

The day-by-day Operations were the most 'tangible' area. Responding to incidents (including SOC teams), forensic activities are daily activities of cybersecurity specialists. The threat intelligence profile was also seen as an operational area, as these professionals work on operational data using multiple sources.

Penetration tester (testing for current and emerging threats), Researcher (bringing new technologies and solutions) and Auditor (identifying gaps) support the Improve stage.

However, since the ECSF is a flexible tool for customised use in a particular context, the CISO **applied the 5-step guide to adapt the role profiles to her specific needs and objectives**. The analysis of the ECSF profiles helped her **define the resource plans** needed to achieve the corporate objective.

In the Plan macro area, she decided to:

- be in charge of policy and compliance tasks to streamline the organisation structure;
- hire a cybersecurity architect who would help to define the overall architecture strategy to cope with cybersecurity risks and ensure secure-by-design solutions to support the digital transformation;

- hire a cybersecurity risk manager who would help assess the corporate cybersecurity risk posture and help define action plans to manage the risks identified.

In the Implementation macro area, she **leveraged the ECSF skills and knowledge components** to **understand what upskilling would be required** to leverage the internal resources available or alternatively decide to hire externally. The multinational corporation had an existing team of instructors in a different field. However, there was no specialist team to design and conduct cybersecurity awareness or trainings courses. The CISO **investigated whether some of the trainers had the skills and knowledge as listed in the ECSF** and the interest **to join her new team**.

In the Operate macro area, the CISO looked at how to manage the day-by-day cybersecurity operations and decided to **set up global security operation centres with incident responders** working on different continents to provide 24/7 support. Moreover, **a threat Intelligence specialist was employed** to provide operational insights to guide hunting for threats and the mitigation of risk. The CISO concluded there was **no need to hire a digital forensic investigator** but rather **engage a specialised consulting company** for any **forensic needs**.

In the Improve macro area, the CISO decided to employ an **external service provider for penetration testing** with the objective of testing the resiliency of the corporate infrastructure and applications. The CISO also assessed the capacity of the internal audit team and decided to **hire a cybersecurity auditor** to audit on security related policies. The CISO did not feel the need to hire a cybersecurity researcher since cybersecurity research was outside the scope of her organisation.

To sum up, Example III highlighted how useful the ECSF can be for the following benefits:

- understanding cybersecurity roles
- assisting in the creation of an organisation structure
- identifying the requirements for cybersecurity roles
- assisting in planning human resources
- upskilling employees
- supporting the assessment of candidates
- using common terminology for collaboration.

Figure 10: Benefits of using the ECSF demonstrated by Example III

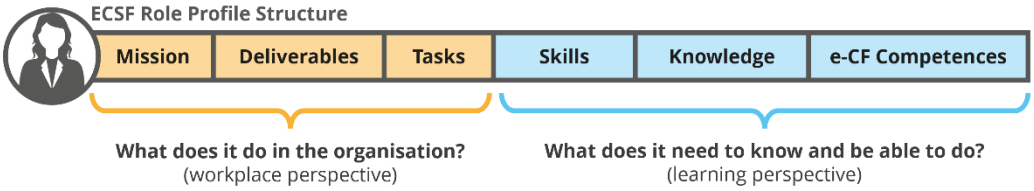
3.2 SKILLING CYBERSECURITY PROFESSIONALS – APPLY THE ECSF AS A LEARNING PROVIDER

The ECSF offers a common language and vocabulary for the development of professional cybersecurity skills to the providers of learning programmes and learning institutions of all types, such as Higher Education (HE), Vocational Education and Training (VET), or any other cybersecurity-related educational programme or training. The defined role profiles provide a cybersecurity workplace-driven, European-embedded approach to link current requirements for professional practice with cybersecurity related curricula and learning programmes.

The ECSF defines the typical requirements of a profile from two fundamental viewpoints.

- What does this role in the organisation do?
  Addresses the workplace perspective (profile sections on mission, deliverables and tasks)
- What does this role need to know and be able to do?
  Address the learning perspective (profile sections on skills, knowledge and e-CF competences)

Figure 11: The ECSF role profiles sections linked to the workplace and learning perspectives



The ECSF positions learning outcomes in a real workplace context. In particular, descriptions in ECSF profiles of roles allow providers of learning programmes to review their curricula in a structured and systematic manner, including from the point of view of practitioners.

The ECSF offers common language and vocabulary for the development of professional cybersecurity skills to the providers of learning programmes and learning institutions of all types.

As illustrated in Annex B.2, the ECSF might contribute to several activities undertaken in academic institutions.

- The ECSF might serve to develop or update the learning outcome of courses and align it to the needs of the job market. The skills, knowledge, and competences within a role profile may be used to guide the design phase of curricula and support the establishment of desired learning outcomes. For example, when analysing the educational needs of a specific cybersecurity job, an aligned ECSF profile provides a solid starting point to understand associated educational requirements.
- The ECSF might serve as a collaboration tool for creating joint academic programmes and for allowing the mobility of students.
- The ECSF might serve as a basis for the definition of a framework for a cybersecurity curriculum which would help universities to map the main focus of their cybersecurity programme and communicate it to the students.

As illustrated in Annex B.1, the ECSF addresses some of the challenges identified in the European cybersecurity professional qualifications landscape. In particular:

- the ECSF supports a cross domain and cross industry agreed terminology related to cybersecurity skills;
- the ECSF might support the development of an integrated platform for skills to provide up-to-date information regarding the job market, competences, training courses, certification schemes and a career roadmap.

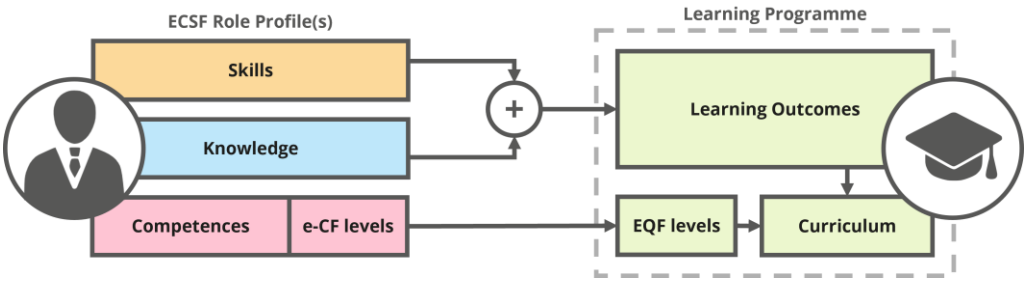
Figure 12: Benefits of using the ECSF as a provider of learning

The ECSF can be used as a communication tool between employers and educators.

In the context of the development of cybersecurity qualifications and curriculum design, the ECSF role profiles serve as a communication tool between employers and educators to improve the consultation process and collaborative outcomes. The employer can quickly define the required activities or tasks and work backwards to identify the competences, skills and knowledge educators should include in curricula. This approach significantly speeds up the design of curricula agreed between employers, governments and educators.

Figure 13 illustrates how the sections of the ECSF role profiles dedicated to competences, knowledge, and skills can be used to define learning outcomes, identify the appropriate levels of learning programmes, and create curricula for cybersecurity occupations. Since knowledge and skills, like all content of role descriptions, are provided as guiding examples for flexible adaptation to the context, other sources may also be used[8].

Figure 13: ECSF profiles guiding cybersecurity professional learning



Connection of learning levels (EQF) and workplace proficiency levels (e-CF)

The European Qualifications Framework (EQF) is a common European reference framework for qualifications. The purpose of the EQF is to compare qualifications and learning outcomes that arise in different countries and national education systems. The EQF is based on the

[8] The skills, knowledge and competences sections of the ECSF are neither exhaustive nor restrictive, allowing the user to enrich them by also including external resources e.g., the Cyber Security Body Of Knowledge (CyBOK) https://www.cybok.org/, JRC Classification https://joint-research-centre.ec.europa.eu/publications/unified-conceptual-framework-tasks-skills-and-competences_en

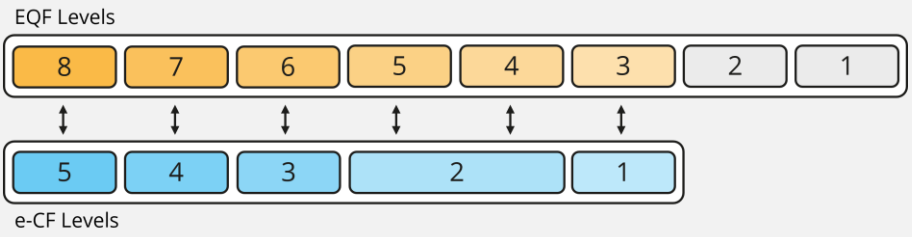
Recommendation on the European Qualifications Framework for lifelong learning adopted by the European Parliament and the Council on 23 April 2008[9].

The EQF defines eight (8) levels of educational attainment with descriptors that differentiate each level. The criterion for each level is based upon assessment of Knowledge, Skills, Responsibility, and Autonomy.

The **European e-Competence Framework (e-CF)**, standard EN 16234-1, used by the ECSF, is a common European framework for ICT Professional competences, knowledge and skills[10]. It relates to competences as needed and applied at the workplace. Dimension 3 of the e-CF defines competence levels originating from workplace proficiency. There are five (5) defined e-Competence levels e-1 to e-5 related to the EQF learning levels 3 to 8 (EQF levels 1 and 2 are not relevant in this context).

The relationship between e-CF levels e-1 to e-5 with the EQF levels 3 – 8 is illustrated below:

Figure 14: Relationship between EQF and e-CF levels



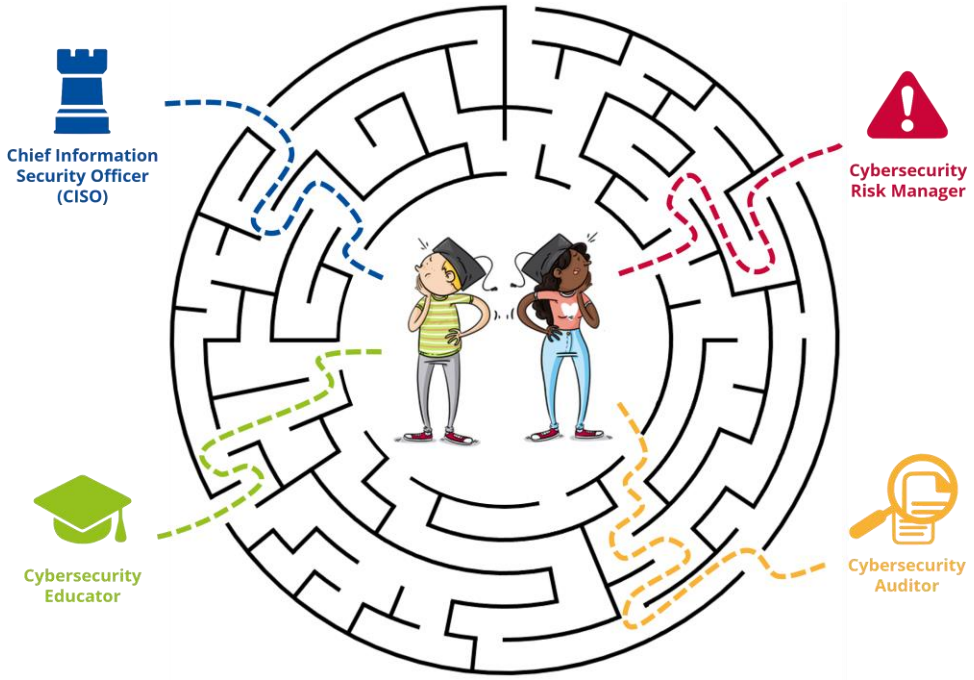
Owing to this systematically developed relationship, it is possible to relate the e-CF proficiency levels with the EQF learning levels. The relationship, due to the different nature of each framework, is not of full equivalence. However, it may be applied to increase transparency and **provide a shared language between requirements for professional competences in the workplace and related qualifications from educational institutions**[11]. Thus, the e-CF competence levels incorporated within the ECSF role profiles can therefore be used as a general guide to required educational levels.

[9] European Qualifications Framework for lifelong learning
[10] EN16234-1:2019: e-Competence Framework (e-CF) – a common European Framework for ICT professionals in all sectors
[11] For further practical guidance see: CEN/TS 17699:2022 Guidelines for developing ICT professional curricula as scoped by EN16234-1 (e-CF)

3.3 MAKING OWN CAREER CHOICES – APPLY THE ECSF AS AN INDIVIDUAL PROFESSIONAL

The common language defined by the ECSF can be used to clear any confusion between professional cybersecurity job roles and cybersecurity educational programmes. By providing a common language and a clear description of the professional job roles in cybersecurity, the tasks expected to be carried out by them as well as the skills, the competences and the knowledge required, the ECSF can build a shared understanding and provide the clarity required to attract new individuals into the cybersecurity field or assist them in planning their career paths.

Figure 15: Using the ECSF to define individual's career paths



The ECSF can build a shared understanding and provide the clarity required to attract new individuals into the cybersecurity field or assist them in planning their career paths.

Professionals already working in cybersecurity related positions can use the ECSF as a guide for advancing in their field. By mapping their skills and knowledge to ECSF role profiles of interest, individuals can identify any missing skills or knowledge that they need to develop, master or learn so that they are ready to cover future job requirements or possible transitions between cybersecurity roles while they progress their professional career. This helps dialogue between employees and employers when planning continuous education within the field of cybersecurity. As the ECSF indicates both formal and non-formal learning paths, it also helps new entrants who are unaware of where to start. Adding to previous knowledge and competences is often an easier pathway than starting completely anew. Annex B.6 deals with this topic, and provides deeper insights and examples in 'individual career decision-making' using the ECSF.

Using the ECSF as a baseline, an individual can identify the required competences and skills to move from one role to another or to identify current training needs.

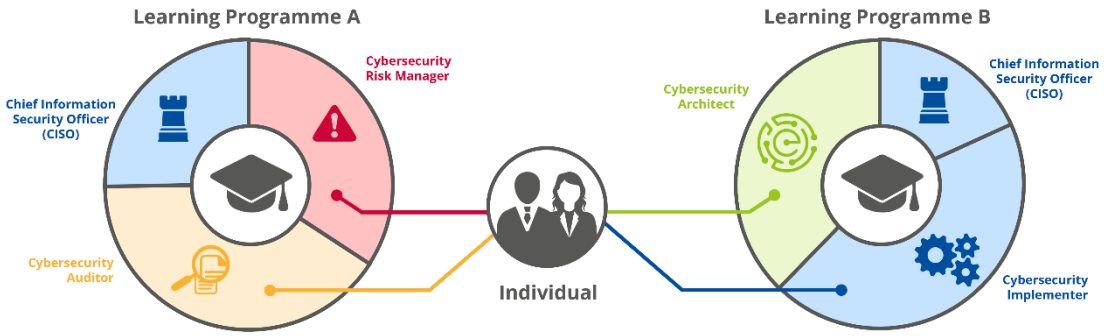
The common language defined by the ECSF can be helpful for individuals looking for cybersecurity jobs. The ECSF can assist in filtering job openings and in understanding the job description while it can also make the job's overall mobility within cybersecurity easier by mapping the individual's skills, knowledge and competences to the ECSF.

Cybersecurity is a good career opportunity even for individuals currently specialised in other fields, hence reskilling people and moving them into the cybersecurity field is a good way to satisfy the workforce needs of the market and reduce the workforce gaps in the field. Since cybersecurity is a multidisciplinary subject, such a career change could be faster for individuals with backgrounds close to one of the main aspects of the field[12]:

- **technical** – related to technology, concrete technological approaches and solutions that can be used to fight against cybercrime and cyberterrorism;
- **human** – related to human factors, behavioural aspects, privacy issues, as well as raising awareness and knowledge of society with regards to cybercrime and terrorism threats;
- **organisational** – related to processes, procedures and policies within organisations, as well as cooperation (public-private, public-public) between organisations;
- **regulatory** – related to the provisions of the law, standardisation and forensics.

By having a clear understanding of the main profiles for cybersecurity roles in the field and a common cybersecurity language across a broader range of sectors as provided by the ECSF, individuals seeking to switch careers towards cybersecurity can use the ECSF as a starting point to identify specific competences skills and knowledge that they need to acquire for the transition.

Figure 16: Using the ECSF to analyse and compare cybersecurity learning programmes



Whether the individual is already working in cybersecurity (looking to expand their knowledge), is currently employed in another field (looking to switch career) or is seeking an academic education (looking to work in cybersecurity in the future), the ECSF can help in understanding the main profiles of cybersecurity roles (by providing a description and analysing them into tasks, skills, knowledge and competences) as well as help in the analysis and comparison of available learning programmes (mapping the learning outcomes to the required skills and knowledge of the cybersecurity profiles of preference).

The ECSF creates a common terminology and shared understanding of the role profiles of cybersecurity professionals, and so it can eliminate confusion in terminology and any lack of understanding

3.4 BUILDING CYBERSECURITY COMMUNITIES – APPLY THE ECSF AS A PROFESSIONAL ASSOCIATION

The ECSF creates a common terminology and shared understanding of the role profiles of cybersecurity professionals. Thus, it can be used by professional associations as a standard to ensure that their work can be used and applied across the EU, eliminating confusion in terminology and any lack of understanding.

Professional organisations can use the framework to conduct market analyses using the ECSF role profiles and present the results in a shared language. For example, the ECSF is expected to be helpful in highlighting the profiles that are lacking in the market, the cybersecurity jobs that

[12] https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity

are in high demand, and the legislative aspects of some professional job profiles. Furthermore, by using the ECSF as a common terminology, professional associations may work towards professional guidance in the cybersecurity sector as presented by Annex B.5.

The use of the ECSF also allows the consolidation of a community of stakeholders to support new developments, improvements and further implementation in EU Member States. Such a framework for collaboration enables human interaction which results in benefits such as knowledge sharing, identification of trends at EU scale, peer-learning activities, application of multidisciplinary approaches and empowerment to adapt and customise the ECSF to specific requirements.

Overall, the ECSF can be used by professional cybersecurity associations as a tool to base their activities on ensuring their EU wide applicability, with the aim of achieving better hardening against cyberattacks across the EU as a society.

3.5 EMPOWERING THE SECTOR STRATEGICALLY – APPLY THE ECSF AS A POLICY MAKER

With the ECSF, a crucial professional community secures clear visibility as using the framework creates a shared understanding of what cybersecurity specialists do. Hence, the ECSF provides a tool to analyse and share critical cybersecurity workforce related collections of data and statistics in a common and EU wide understandable terminology. Such data are important for policymakers as they obtain better insights of the state of the cybersecurity workforce across the EU, thus enabling them to understand and estimate the future needs of cybersecurity specialists in quantity and quality. Such strategic input helps to update and maintain the ECSF itself, so that its relevance in the future remains valid. Furthermore, by defining a common terminology, the ECSF allows for cross border collaboration between policymakers through data and information sharing.

Given a structured approach to a very diverse market environment, the ECSF role profiles provide a valuable tool for the support of policymakers, market surveyors and other stakeholders with the influence and role to empower the sector strategically.

Given a structured approach to a very diverse market environment, the ECSF role profiles provide a valuable tool for the support of policymakers, market surveyors and other stakeholders with the influence and role to empower the sector strategically. The ECSF Profiles can be helpful for data studies on supply and demand carried out at national, European and international levels. The profiles provide a shared, agreed definition to facilitate the collection of reliable and comparable data in the cybersecurity job market, including the supply and demand for different types of cybersecurity professionals and related requirements for particular skills.

Policy-making processes addressing cybersecurity can benefit from data collection at the time of making decisions, e.g. funding provisions, investment priorities and periods of intervention. Besides the core activities of each profile, the activities carried out by them may contribute to generating and gathering relevant data sets that can support policy decisions. Annex B.3 shows how fragmented information constitutes a challenge when making decisions and the actions INCIBE is taking in addressing this challenge with the support of the ECSF. By incorporating the ECSF as a homogeneous framework for the definition of cybersecurity profiles, EU member states get valuable support in achieving their objectives of increasing cybersecurity talents and becoming aligned with the rest of the countries at the European level.

4. TERMS AND DEFINITIONS

Term	Definition	Source
cybersecurity	Any activity necessary to protect network and information systems, the users of such systems, and other persons affected by cyberthreats.	ENISA mandate (Regulation (EU) 2019/881)
cyberthreat	Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.	ENISA mandate (Regulation (EU) 2019/881)
Information and Communication Technology	ICT stands for Information and Communication Technology. It is used in many different contexts and from a technical point of view ICT relates to digital computers and internet (communication) systems, including software, hardware and networks. From an economic and political standpoint, ICT relates to a cross sector of enterprises, including manufacturers, product suppliers or service providers relating to the ICT field.	EN16234-1:2019 e-Competence Framework (e-CF)
competence	The demonstrated ability to apply knowledge, skills, and attitudes to achieve observable results. Examples are B.1. Application Development and E.3. Risk Management.	EN16234-1:2019 e-Competence Framework (e-CF)
skill	The ability to carry out managerial or technical activities and tasks on a cognitive or practical level; knowing how to do it.	EN16234-1:2019 e-Competence Framework (e-CF)
soft skills	Interactive skills used to engage successfully with situations in the workplace; may refer to work quality, social interaction, or emotion. (also called transversal, transferrable, or behavioural skills)	EN16234-1:2019 e-Competence Framework (e-CF)
knowledge	Body of facts to be applied in a field of work or study; knowing what to do.	EN16234-1:2019 e-Competence Framework (e-CF)
attitude	Representation of the human element of an e-competence; it reflects on how a person integrates knowledge and skills and applies them appropriately in context.	EN16234-1:2019 e-Competence Framework (e-CF)
learning outcome	Statement of what a person knows, understands and can perform on completion of a learning process	European Qualifications Framework (EQF)
role profile	An outline or general document that demonstrates the relationship between specific activities or tasks in a role and the individual skills, competences and knowledge required to undertake them. Unlike a particular job, a role derives from an	Creative Leadership – Talent Management CWA ICT Profiles

	organisational need to do something. Assigned employees can meet organisational requirements by carrying out all or part of the tasks required to ensure their role.	
job profile	A context-specific and detailed description of what an employee does to assure that the job holder has no doubts about their tasks, duties, responsibilities and often those to whom they report. It usually contains precise information about the competences, skills and knowledge required and practical information about health and safety and remuneration.	ICT Profiles CWA
proficiency level	A clear indication of the degree of mastery that allows a professional to meet requirements in the performance of a competence. EN 16234-1 (e-CF) incorporates proficiency levels e-1 through to e-5. The e-CF characterises proficiency levels by combining levels of influence within a community, context complexity, and autonomy.	EN16234-1:2019 e-Competence Framework (e-CF)
learning level	Indicates a grading and may be represented by a formal qualification. Learning levels generally derive from an education system or indicate a grading in a taxonomy of intellectual or learning behaviours (such as memorising, applying, interpreting) and have a relationship with proficiency levels but are to be distinguished from these.	EN16234-1:2019 e-Competence Framework (e-CF)

5. REFERENCES

ENISA Mandate, Regulation (EU) 2019/881, https://eur-lex.europa.eu/eli/reg/2019/881/oj

European ICT Professional Role Profiles, CWA 16458
https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:67523,412798&cs=1799176DA0D15C74D91B71423CAD4A9A3

EN 16234-1:2019 e-Competence Framework (e-CF), A common European Framework for ICT Professionals in all sectors

CEN/TS 17699:2022 Guidelines for developing ICT Professional Curricula as scoped by EN 16234-1 (e-CF)

CEN/TS 17834:2022 European Professional Ethics Framework for the ICT Profession (EU ICT Ethics)

European Qualifications Framework (EQF)

ESCO The European multilingual classification of Skills, Competences and Occupations, http://www.ec.europa.eu/esco

IFIP Code of Ethics

NIST Incident Response Lifecycle

The National Initiative for Cybersecurity Education (NICE) by the National Institute of Standards and Technology in the US

National Cybersecurity Strategies (NCSSs), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools

The Cybersecurity Body of Knowledge (CyBOK) by the UK National Cyber Security Programme and the University of Bristol, https://www.cybok.org

JRC, Taxonomy and glossary for Cybersecurity by European Commission, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

The European Skills Agenda, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1196

Digital Education Action Plan, https://education.ec.europa.eu/focus-topics/digital-education/about/digital-education-action-plan

Pact for Skills, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197

Leading the Digital Decade, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197

ENISA, Forensic Analysis, Webserver analysis, Handbook, Document for teachers, 2016, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe3_forensic_analysis_iii-handbook

Council of Europe, Electronic Evidence in Civil and Administrative Proceedings, Guidelines and explanatory memorandum, 2019, https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

A ANNEX: CONNECTING THE ECSF TO OTHER EU STANDARDS AND FRAMEWORKS

The ECSF is a framework to support the professional cybersecurity domain in the EU. Connecting existing recognised European structures of relevance to the EU's professional cybersecurity domain was a vital ECSF design principle (see section 2.1)

The following paragraphs provide a brief overview of the main standards and frameworks to which the ECSF is connecting.

A.1 EN16234-1 E-CF A COMMON EUROPEAN REFERENCE FRAMEWORK FOR ICT PROFESSIONALS IN ALL SECTORS

The European Norm (EN) 16234-1 European e-Competence Framework (e-CF) provides a reference of 41 competences as applied in the information and communication technology (ICT) workplace using a standard European language for competences, skills, knowledge and proficiency levels that can be understood across Europe. The prime objective of this standard is to provide a common European language for ICT workplace-related competences, skills, knowledge and proficiency levels as required and applied by organisations and professionals. In this way, all sector stakeholders, including the public and private sectors and individuals, have access to a shared reference.

The standard was established as a tool to support mutual understanding and provide transparency of language through the articulation of competences required and deployed by ICT professionals. This standard is structured across multiple dimensions. The dimensions reflect areas of business and human resource planning and incorporate job and work proficiency guidelines. In addition, this standard adds a transversal component which provides basic generic ICT descriptors for successful application of e-CF competences in the context of a workplace.

Table 4: EN16234-1 (e-CF) overview. Source: CEN 2019

Dimension 1 5 e-CF areas	**Dimension 2** 41 e-Competences identified	**Dimension 3** 5 e-Competence proficiency levels				
		e-1	e-2	e-3	e-4	e-5
A. Plan	A.1. Information Systems and Business Strategy Alignment					
	A.2. Service Level Management					
	A.3. Business Plan Development					
	A.4. Product/Service Planning					
	A.5. Architecture Design					
	A.6. Application Design					
	A.7. Technology Trend Monitoring					
	A.8. Sustainability Management					

	A.9. Innovating					
	A.10. User Experience					
B. Build	B.1. Application Development					
	B.2. Component Integration					
	B.3. Testing					
	B.4. Solution Deployment					
	B.5. Documentation Production					
	B.6. ICT Systems Engineering					
C. Run	C.1. User Support					
	C.2. Change Support					
	C.3. Service Delivery					
	C.4. Problem Management					
	C.5. Systems Management					
E. Enable	D.1. Information Security Strategy Development					
	D.2. ICT Quality Strategy Development					
	D.3. Education and Training Provision					
	D.4. Purchasing					
	D.5. Sales Development					
	D.6. Digital Marketing					
	D.7. Data Science and Analytics					
	D.8. Contract Management					
	D.9. Personnel Development					
	D.10. Information and Knowledge Management					
	D.11. Needs Identification					
E. Manage	E.1. Forecast Development					
	E.2. Project and Portfolio Management					
	E.3. Risk Management					
	E.4. Relationship Management					
	E.5. Process Improvement					
	E.6. ICT Quality Management					
	E.7. Business Change Management					
	E.8. Information Security Management					
	E.9. Information Systems Governance					

The e-CF provides consistent links in the context of ICT qualifications and other frameworks of relevance to the sector (in particular, EQF, DigComp, European ICT Professional Role Profiles, behavioural skills, ESCO, EQANIE, SFIA, Foundational Body of Knowledge for the ICT Profession, ISO and other ICT industry standards).

For each cybersecurity role, a set of applicable e-CF competences was selected at the application level as an incorporated element of the profile description for the role of cybersecurity professional.

A.2 EUROPEAN ICT PROFESSIONAL ROLE PROFILES

The CWA 16458 European ICT Professional Role Profiles provides a generic set of typical roles performed by ICT Professionals in any organisation, covering the entire ICT business process. Thirty profiles in total provide a sound starting point and inspiration for the creation of more context-specific and flexible profiles based upon organisational roles, individual job descriptions or sub-domain specialisations from various contexts. By applying e-CF competences to the construction of ICT profiles, the European ICT Professional Role Profiles also provide a tool and entry point for e-CF application to individuals and organisations who wish to work with the e-CF.

The European ICT Professional Role Profiles are described by using a consistent format incorporating the following elements: a summary statement, a mission statement, deliverables, main tasks, e-Competences, and Key Performance Indicators (KPI) areas[13].

By adopting the most suitable elements of the European agreed and practice-driven ICT Profile description scheme, the ECSF profiles become comparable and provide a unique, easily accessible and comprehensive overview of the requirements for European cybersecurity professionals.

These detailed high content profiles have loose links to the generic roles incorporated in the overall European ICT Professional Profile set. From the ECSF user perspective, confidence can be established in the sustainability of the structure through its association with European ICT Profiles but with focused application for the cybersecurity community.

A.3 EUROPEAN QUALIFICATIONS FRAMEWORK

The EU developed the **European Qualifications Framework (EQF)** as a translation tool to make national qualifications easier to understand and more comparable. The EQF seeks to support cross-border mobility of learners and workers, and to promote lifelong learning and professional development across Europe.

The EQF is an 8-level, learning outcomes-based framework[14] for all types of qualifications. It serves as a translation tool between the various frameworks of national qualifications. This framework helps improve transparency, comparability and portability of people's qualifications and makes it possible to compare qualifications from different countries and institutions.

The EQF covers all types and all levels of qualifications and the use of learning outcomes makes clear what a person knows, understands and is able to do. The level increases according to the level of learning, with level 1 the lowest and 8 the highest level. Most importantly the EQF is closely linked to national qualification frameworks[15], so it provides a comprehensive map of all types and levels of qualifications in Europe, which are increasingly accessible through qualification databases. The EQF was set up in 2008 and later revised in 2017[16].

The ECSF profiles contain e-CF competences and e-CF level assignments, which provide a consistent link with EQF levels (see section 3.2). This orienting relationship provides a bridge in understanding between the provision of learning programmes and workplace requirements.

A.4 ESCO - EUROPEAN CLASSIFICATION OF SKILLS, COMPETENCES AND OCCUPATIONS

ESCO is the multilingual classification of European skills, competences, qualifications and occupations. The key purpose of ESCO is to provide a dictionary, describing, identifying and classifying professional occupations and skills relevant to the EU labour market, education and training and systematically showing the relations between those occupations and skills. ESCO is managed by the European Commission, which is responsible for updating the classification. The ESCO resource supports two of the EU's key strategies in the field, Europe 2020 and Skills Agenda for Europe[17].

[13] CWA 16458 European ICT Professional Role Profiles
[14] https://europa.eu/europass/en/description-eight-eqf-levels
[15] https://europa.eu/europass/en/national-qualifications-frameworks-nqfs
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&from=EN
[17] https://ec.europa.eu/social/main.jsp?catId=1326&langId=en

The goal of ESCO is to describe all occupations in the European labour market, thus including cybersecurity. It is therefore useful to establish an orienting mapping between the ECSF role profiles and some of the ESCO profiles.

On Table 5, several cybersecurity related ESCO Occupations are listed along with an indicative mapping to ECSF role profiles. Since the relationship between them is not always one- to-one, the following relationships were defined to explain the corresponding connections:

- **is** – This ESCO Occupation can be mapped to the corresponding ECSF role profile as both describe the same cybersecurity role.
- **might include** – This ESCO Occupation may include, based on the context, the ECSF role profile listed. (This is an indicative mapping.)
- **might be included** – Some aspects of this ESCO Occupation may describe parts of the ECSF role profile listed. (This is an indicative mapping.)

Table 5: The ESCO profiles and the ECSF profiles relationships

ESCO code	ESCO Occupation	Relationship	ECSF role profile
2149.2.8	Research engineer	might include	Cybersecurity Researcher
2310.1	Higher education lecturer	might include	Cybersecurity Educator
2356	Information technology trainer	might include	Cybersecurity Educator
2511.18	IT auditor	might include	Cybersecurity Auditor
2519.2	ICT auditor manager	might include	Cybersecurity Auditor
2529.1	Chief ICT security officer	is	Chief Information Security Officer (CISO)
2529.2	Digital forensic expert	is	Digital Forensics Investigator
2529.3	Embedded system security engineer	might be included	Cybersecurity Implementer
2529.4	Ethical hacker	is	Penetration Tester
2529.6	ICT Security administrator	might be included	Cybersecurity Implementer
2529.7	ICT security engineer	might be included	Cybersecurity Architect
2529.7	ICT security engineer	might be included	Cybersecurity Implementer
2619.4	Data protection officer	is	Cyber Legal, Policy & Compliance Officer

Important note: The relationship between the ESCO occupation and the ECSF role profile does not represent an equivalence; it offers a best fit approximation that readers may wish to investigate.

B ANNEX: USE CASES

A use case shows why and how an organisation is using the ECSF, emphasising the variety of approaches and benefits. This annex is a collection of cases that were publicly available on 20 July 2022.

The following use cases are merely illustrative examples. The Information and contents included in these cases should not be considered as an endorsement or validation statement from ENISA. The use of these examples should be seen as inspirational cases rather than as conditioning baselines or benchmarking references.

B.1 USE CASE FROM CONCORDIA H2020 PROJECT

This section includes parts from the use case written by CONCORDIA H2020 project[18].

Towards an integrated platform for skills in cyber built on the European Cybersecurity Skills Framework

Difficult to understand the trainings big picture

The needs to protect oneself against threats to information and operations, to maintain the cybersecurity posture of an organization and to increase the resilience against such threats, are still urgently felt by all interested parties. A core component to fulfilling these needs, is the existence of cyber – competent professionals. And competence regarding cybersecurity is not only needed for the dedicated professionals (external or internal to an organization) but also for all staff members of an organization even if they are not directly involved in cybersecurity processes and activities.

When it comes to the cybersecurity professionals, various publications still report a cybersecurity skills gap, flagging that the top 3 competencies missing or not enough covered by the existing professionals varies from one year to another[19]. On the other hand, a considerable amount of Cybersecurity related courses and trainings are offered by various European and international organisations. A simple search on the internet will reveal many courses that relate to the cybersecurity domain, without providing a clear picture on the competencies offered or how they could relate to a specific role. To add to this confusion, there are training courses that seem to address one specific role (e.g. CISO), have similar titles but have different curriculum.

Hence, in several cases, the information provided is confusing the trainee on what and how they should perceive cybersecurity concepts, as well as how to use them to cover their professional needs. Besides, the courses for professionals are promoted on a variety of platforms and they are difficult to be compared with respect to the competencies covered and role profile addressed. This makes difficult for an individual to build a clear career path and identify development opportunities.

[18] https://www.concordia-h2020.eu/blog-post/towards-an-integrated-platform-for-skills-in-cyberbuilt-on-the-european-cybersecurity-skills-framework/
[19] https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/state-of-the-cybersecurity-workforce-new-isaca-research-shows-retention-difficulties-in-years

The CONCORDIA map of courses for cybersecurity professionals

In an attempt to address these challenges, we have built the CONCORDIA map of courses and trainings for cybersecurity professionals[20]. The map is displaying structured information on existing European offer for short courses/trainings and provides different filters as to help match easier the specific need for skills development with the offer. [...]

One can choose to sort the courses based on the cybersecurity level addressed (Device-, Network-, Software/ System, Data/ Application-, User-Centric), or on the relevance to an industry sector (e.g. Telecom, Financial, Transport e-mobility, e-Health or Defence), but also on the format (face-to-face, online, blended), and the timing of the course/training.

Missing a key ingredient – Solution enabled by ECSF

Although we are offering on the CONCORDIA map a large plethora of filters to help the users identify easier the course(s) of interest, the database lacks a key ingredient – the links to role profiles that each of the courses are addressing through the knowledge and skills covered. The e-CF European Competence Framework for ICT professionals available at the time of building the map defines 30 role profiles and 40 associated competencies but they are difficult to be associated to the specificities of the cybersecurity domain.

This was a challenge of the cybersecurity education ecosystem we flagged already two years ago and captured in the CONCORDIA Roadmap for Education[21] under the heading C5: Heterogeneity of competencies related terminology. This lack of a cross-domain and cross-industry agreed terminology related to the cybersecurity skills necessary for a specific role makes it difficult for companies to fill in open positions. They find it hard to match the recruitment criteria with the studies and the qualifications listed in the CVs of the applicants because of the use of non-standard terminology. Individuals, in turn, cannot easily identify the skills they need to possess or develop to match market demand. And, finally, course providers have difficulties in designing curricula that answer to the market needs.

As part of the CONCORDIA roadmap, we pledged for one single platform hosting all the existing Cybersecurity related programs (university level and Ph.D. programs, short courses and trainings for professionals). [...]

The platform should consider collecting the content by using categories based on a standard terminology (specific skills framework included). The categories would be further used as filters for different enquires of the courses database. The 12 role profiles defined in the current version of the European Cybersecurity Skills Framework (ECSF) seem to be a natural solution.

The benefit for stakeholders

The adoption of a standard lexicon such as the one proposed by the ESCF, including cybersecurity role profiles will help companies identifying the right talent for the jobs as well as education providers to better shape their curriculum to match the cyber workforce needs. By applying the same terminology and using an EU wide skills framework to job descriptions, course description and role profile would help individuals selecting the right education modules to support their career path, and filtering better the jobs openings according to their competence and level of expertise. Finally, the policy makers would be able to collect more structured data at country/regional level in support of future policy development and have a solid basis when coordinating with external countries towards addressing global scale cyber security challenges.

[20] https://www.concordia-h2020.eu/map-courses-cyber-professionals/
[21] https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf

Towards an integrated platform for skills

Building on the CONCORDIA database of courses and trainings for cybersecurity professionals, the REWIRE project[22] attempts to make further steps towards integrating the relevant cybersecurity skills related content. The REWIRE CyberABILITY platform – currently in design phase – will provide up-to-date information regarding the job market, competences, training courses, certification schemes and a career roadmap.

B.2 USE CASE FROM SPARTA H2020 PROJECT

This section includes parts from the use case written by SPARTA H2020 project[23].

Improving higher education using ECSF and SPARTA Curricula Designer

Introduction

This use case provides recommendations on how ECSF can be used to shape education programmes that are linked with cybersecurity. As ECSF manifests the structure of high-level profiles from practitioners' point of view, including main tasks, relevant knowledge and skills, this can provide more focused approach for building specialized and comprehensive study programs, tailored to specific profiles, instead of covering cybersecurity in general.

Challenge

Education institutions compose their curricula considering the complete path – starting with the fundamental courses that are required for the student to learn as a basis for the next set of follow-on courses, which are often cybersecurity-specific. However, the selection of courses to be included in the cybersecurity curricula is up to the institution.

Each education institution has its own specific environment (determined by, e.g., infrastructure, equipment, expertise of teachers, composition of existing programs, etc.) and there is no universal way how the curriculum should be constructed.

Education providers differ in what concrete subdomain of cybersecurity they would like to focus on. Some providers are very technical, focusing on, e.g., computer science, some more social-oriented, focusing on legal and societal aspects. Therefore, the interoperability among the resulting study programs and a common language is currently a significant challenge.

Some academic programmes do not build skills and competencies that prepare students for specific work roles available on the job market. This poses a challenge for students which do not understand what are the occupational possibilities at the end of their studies.

Solution enabled by ECSF

The ECSF may contribute to the following activities that address challenges above:

- Evaluation: Description of profiles allows institutions to review their curricula in a structured and systematic manner, understanding the practitioners' point of view. This allows to understand for what profile institution is mainly targeting their graduates.

[22] https://rewireproject.eu/

[23] https://sparta.eu/assets/pdf/ECSF%20Training%20and%20education%20use%20case%20with%20SPARTA%20Curricula%20Designer.pdf

- Improvement: Can be done based on the evaluation exercise. This is especially important considering the set of knowledge / skills ascribed to specific profile.
- Focus: Education provided by universities may differ in the way they address core competencies. Some might be more focused on specific technological courses, some on law, others on forensics, etc. Having an ECSF to work with, they can map their core competencies onto various courses areas, important for defined profiles. This enables the institution to develop more effective targeted programs in house around the main competencies.
- Collaboration: ECSF gives the education providers the common language and vocabulary for describing their courses, creating joint programmes and allowing mobility of students.

While applying ECSF to cybersecurity education, the following approach is recommended:

- Courses in curricula can be classed as belonging to either Fundamental or Cyber Security categories. Fundamental courses are those that might not be directly linked to the ECSF, but which serve as a prerequisite for later studies. For example, Fundamental Cryptology is the prerequisite for Cryptanalysis or Advanced Cryptology; Number Theory is necessary for most intermediate and advanced computer related courses.
- Once the Fundamental courses are identified, the Cybersecurity courses can be proposed to address requirements of work roles the students are aiming to. Linking is achieved based on the content of individual courses, which can be linked to the profiles and finally to work roles. The concrete steps, [...], are:
    a. For a specific Work Role 1, education providers find the relevant Profiles (Profile 1 and Profile 12 in our example). This mapping, marked by brown arrows, should be specified by the job advertisers/employers.
    b. Education providers identify the necessary knowledge and skills for selected profiles. These requirements are defined by the ECSF, marked by blue arrows.
    c. Education providers design new or reuse existing courses (in our example courses 1, 2, 3, 4) that address the knowledge and skills identified in the step above. This mapping between courses and their content must be done by course administrators.
    d. Having all necessary courses (and all prerequisites for them, general non-cybersecurity courses, other courses for broadening the scope of students, etc.), the core of the curriculum is ready.
- Of course, the ECSF can be applied also in an exactly opposite way: first composing the curriculum from individual courses, analysing the knowledge and skills provided, using the ECSF to identify profiles and, finally, finding the work roles that are supported by the curriculum. This mapping reveals what exact knowledge and skills is already present in the curricula or, on the other side, what is missing and should be stressed or added to the courses. In this way, the ECSF helps to structure the curricula for a better fit with the expected profiles and job roles.

Result / added Value by SPARTA

SPARTA project used a cybersecurity skills framework to create a free tool called Cybersecurity Curricula Designer. It is a simple web application that helps education providers to create new study programs on cybersecurity and/or to analyze existing study programs according to their content and its reflection of cybersecurity jobs requirements.

The tool [...] allows study program administrators to compose their study program by dragging and dropping courses from the left section to the middle section. Courses, from which

administrators develop the study programs, can be either pre-defined or custom. While composing the study program, the statistical data about its content is displayed in the right section. Besides other data, the information about what competencies and work roles are supported by the program are provided. By using the tool, it is easy to find out what content is missing in the study program and what specific work roles are best-suited for the graduates of the program. In this case, the cybersecurity skills framework is the core of the applications which allows linking the skills and knowledge with job roles. [...]

B.3 USE CASE FROM INCIBE

This section includes parts from the use case written by INCIBE[24].

Use case from INCIBE

Introduction

The effectiveness in protecting a country depends largely on the capabilities of its people, and estimates in this regard are that by 2022, Spain could reach a cybersecurity workforce of close to 122,284 workers with a talent gap estimated at 24,119. Consequently, one of the top priorities for the administration today is to meet the challenge of identifying, attracting, developing, and retaining talent in the various fields of cybersecurity.

Proof of this commitment is the development of the Spanish government's 2019 National Cybersecurity Strategy[25], which emphasizes the need not only to have a defense and protection position for companies and citizens, but also to support the boosting of the cyber industry, recognizing the key role that cybersecurity plays in the current environment of transformation and uncertainty and the opportunity it offers to increase Spain's competitiveness. Aligned with objective 4 of the Strategy, action line 5 highlights the importance of boosting the Spanish cybersecurity industry, in addition to the generation and retention of talent for the strengthening of digital autonomy.

On the other hand, the Digital Spain 2025 Plan[26] seeks to reinforce the levers that will facilitate a return to the path of economic growth, and one of its strategic axes is to strengthen Spain's cybersecurity capacity to mitigate risks and increase confidence in the path towards a digital and sustainable economy.

In its strategic axis 4, dedicated monographically to cybersecurity, it incorporates the measures that make up INCIBE's three main lines of action for the coming years: increasing the cybersecurity capabilities of citizens and companies; boosting the Spanish cybersecurity ecosystem around its industry, R&D&I and cybersecurity talent; and consolidating Spain as an international node in the sector. Spain Digital 2025 already recognizes the key role of cybersecurity talent as a driving force for the sector.

These national initiatives generate a suitable scenario that favors research, innovation, and involves the most relevant agents of the value chain, such as educational institutions and organizations, so that they see the benefit of managing the knowledge, capabilities and technological experiences that respond to the great challenges that the country has in terms of cybersecurity.

[24] http://www.incibe.es/en/talento-hacker/publications/european-cybersecurity-skills
[25] https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
[26] https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx

For its part, the Spanish National Cybersecurity Institute (INCIBE), a company under the Ministry of Economic Affairs and Digital Transformation, through the Secretary of State for Digitalization and Artificial Intelligence; and the reference entity for the development of cybersecurity and digital trust of citizens and companies, and of the Spanish academic and research network (RedIRIS), has the mission of improving cybersecurity and digital trust of citizens, minors and private companies in Spain.

In addition, its mission includes the protection and defense of these groups, the promotion of Spanish industry and R&D&I in cybersecurity, as well as the identification, generation and attraction of talent to the cybersecurity sector.

Cybersecurity talent is, therefore, a cornerstone of INCIBE's actions. Without talent it is impossible to develop a strong industry or the high value-added solutions needed to participate in a highly competitive market such as cybersecurity.

However, the information available so far on the state of talent in the cybersecurity sector in Spain was varied and fragmented, coming from different sources, which hindered the deep understanding of the environment necessary to channel actions. [...]

That is why, with the aim of offering a clear vision of cybersecurity talent in Spain, INCIBE publishes in March 2022, the results of an analysis and diagnosis of cybersecurity talent at national level, whose process has been carried out through rigorous analytical premises, global work approach and participatory and inclusive processes that have taken into account the main actors of the cybersecurity ecosystem. [...]

Challenge

The recommendations derived from this analysis project are the starting point for ensuring a robust and profitable cybersecurity industry that is characterized by putting people talent at the core of initiatives. In this sense, the entire cybersecurity value chain can see this study as an opportunity to further connect with and better understand the cybersecurity talent in Spain.

It is therefore necessary to structure and implement effective practices that impact the management of this specific type of talent in organizations. The importance of cybersecurity for the survival of organizations requires the need to address the problem of identifying this type of specific talent in cybersecurity, the evolution of the recruitment and on boarding process, as well as the adoption of actions that contribute to improving management and mitigating talent drain.

For this reason, the promotion of national policies, coordinated from the administration that focus on strengthening and promoting initiatives to make cybersecurity a strategic priority in organizations, as well as structuring and structuring a training itinerary for the performance of cybersecurity as a professional activity are priorities on which both organizations and recruitment companies will establish in their actions for the identification, attraction, recruitment and management of cybersecurity talent.

In this way, a set of recommendations are established that this type of agents (Public Administration, recruitment companies and other organizations) could implement to increase cybersecurity talent in Spain and that set the starting point to solve the challenges that lie ahead in this regard. [...]

Solution enabled by ECSF

There are several factors (political, economic, social, technological, legal, etc.) that can impact the cybersecurity industry, and consequently, the shortage of talent, gaps and in general a mismatch between supply and demand.

One of these relevant factors in the European Union, is the lack of standardization of the definition of cybersecurity roles and skills associated with those roles.

Provide a basis for continuous communication between different stakeholders (government, industry, academia, policy makers and citizens).

This type of tool serves as a basis for a more competent and complete workforce that understands the same language as other professionals at the European. [...]

Result / added Value

Therefore, in the context presented, two initiatives have been launched at the national level, which will give value to the ECSF developed by ENISA and which will be very useful. [...]

Both initiatives, coordinated with each other, will incorporate the ECSF as a homogeneous framework for the definition of cybersecurity profiles, which will allow Spain to achieve its talent objectives and be aligned with the rest of the countries at European level. [...]

B.4 USE CASE FROM THE EUROPEAN CYBER SECURITY ORGANISATION (ECSO)

This section includes parts from the use case written by the European Cyber Security Organisation (ECSO)[27].

Towards a harmonised education approach with the European Cybersecurity Skills Framework (ECSF)

Having worked on education, training and skills in its WG5 since 2016, ECSO has seen first-hand the challenges posed by the fragmentation and scattered approaches that exist within cybersecurity today. In this blog post, ECSO reflects on the existing European approaches to education and up-skilling and focuses on ENISA's European Cybersecurity Skills Framework (ECSF).

Education is not only a national prerogative. It is it also inherently linked to collaboration between national entities, the wider cybersecurity community and European bodies. With this in mind, collaboration is key when coming up with pan-European approaches to harmonise cybersecurity education curricula and tackling the skills or, more concretely, the workforce gap. There is ample opportunity to leverage the collaborative spirit of the European cybersecurity community to deliver practical solutions and initiatives that can have an impact "on the ground", and ENISA's European Cybersecurity Skills Framework (ECSF) can play a big part in this respect.

Cybersecurity education: an ECSO perspective

From the perspective of the European Cyber Security Organisation (ECSO), as representative body of the European cybersecurity public-private ecosystem and community), the potential

[27] https://www.ecs-org.eu/newsroom/consolidated-educational-and-recruiting-scheme-the-glue-to-fix-todays-scattered-approach

value of the ECSF is non-negligible when it comes to linking existing efforts, providing foundational elements for a European cybersecurity workforce, and delivering a common framework and taxonomy for the application of profiles and skills. Cybersecurity professionals, education & training providers, policy makers, and recruitment professionals, alike, stand to gain from the wider implementation of the ECSF.

The Challenge

It is evident that there is a growing need for a skilled cybersecurity workforce. Various studies across the globe from industry and academia confirm that the cybersecurity workforce demand is very high and that it is difficult to hire competent professionals. The 2021 edition of the annual Cybersecurity Workforce Study published by ECSO Member (ISC)[228] states that the shortage of cybersecurity professionals is 2.72 million globally which, although having decreased from 3.12 million the year prior, is still a significant number. While these studies offer a basis upon which to assess the global situation, the reality is that it is very difficult to quantify the extent of the cybersecurity talent shortage in Europe. We know that the demand for experts will inevitably rise due to the growth of the cybersecurity market and regulatory landscape, leaving an urgent gap to fill with more (and different kinds of) experts. [...]

But it is not only a matter of numbers. Through a recent ECSO study on HR recruitment practices and trends, ECSO has also observed an increase in the time it takes, on average, for organisations to fill their cybersecurity positions. Many organisations indicate that it may take up to six months for the recruitment process, which is slower than in order knowledge domains, while others state that they have difficulties with filling their cybersecurity positions altogether. This clearly indicates that there is a mismatch between the supply and demand (i.e. gap between academia and industry requirements) and push/pull factors (i.e. candidate suitability and assessment, attraction to jobs and benefits). However, the main issue for employers remains the general lack, worldwide, of cybersecurity specialists, while the demand is constantly growing. Several organisations also highlight the complexity of hiring experts for a domain that they do not master. ECSO's survey also indicated that, as a growing trend, several candidates, despite lacking significant cybersecurity skills, still enrich their CV with cybersecurity concepts and keywords.

These challenges clearly highlight the need for a common language to support recruitment efforts and the importance of considering the multidisciplinary nature of cybersecurity that is so unique to the field vs the more traditional IT/ICT professions. While existing frameworks such as NICE, CyBoK, and eCF provide useful guidelines for skills development, a European framework that provides an overarching profile taxonomy and career pathways inherent to cybersecurity, has been missing. The release of the ECSF is therefore very timely and fundamental to supporting the European cybersecurity community in attracting, skilling, and re-skilling experts.

There is a solution

ECSO will apply the ECSF in a number of ways to boost its uptake and leverage its potential to harmonise cybersecurity education and skills across Europe.

ECSO will:

- Map out its Minimum Reference Curriculum to the ECSF, giving course designers and practitioners a first-hand look at how best to define their curricula towards dedicated career pathways. This will help ensure that university courses adequately reflect the realities of the needs of the cybersecurity job market while allowing for a continuous updating of the curriculum.

[28] https://www.isc2.org/Research/Workforce-Study

- Use the ECSF and associated use manual to support HR/recruitment in the drafting of job advertisements and organisation of practical skills assessment/evaluation procedures. We will also conduct a follow up HR survey using the ECSF job profiles to understand what roles are most needed by organisations and progressively build up a quantitative understanding of the European cybersecurity job market.
- Use the ECSF as base taxonomy for two dedicated platforms envisaged by the Women4Cyber Foundation and ECSO [...]

Result and added value

The added value of the ECSF for the European cybersecurity community is first to have a common framework and taxonomy upon which to work. This will lead to a better understanding of the skills needs and the practical realities of different job profiles, which will enhance the cybersecurity workforce, not only through more efficient recruitment and retention measures, but also through facilitating the entry or re-entry of more women and other underrepresented groups (i.e., the neurodiverse) into the field. The ECSF, in highlighting the technical and non-technical aspects of different profiles, will contribute to removing the misconception that cybersecurity is only a technical topic, when it is as much about people and processes. In this respect, emphasising the importance of soft (transferable) skills in the domain will contribute significantly to attracting more women into the cybersecurity profession. The ECSF will also reduce the fragmentation of approaches by introducing top-down guidelines for how to categorise the multifaceted nature of the cybersecurity profession. The profiles proposed by the ECSF are sufficiently broad to be able to underpin the many roles that the profession has to offer while being segmented in a way that makes it understandable and applicable for practitioners, industry experts, policy makers, recruitment specialists and job seekers alike.

At ECSO, we are convinced that the ECSF will provide significant value to our work and support the wider community with a concrete tool for harmonising efforts and bridging the gap between the demand and supply of experts.

B.5 USE CASE FROM ISC2

This section includes parts from the use case written by the (ISC)²[29].

Using the (ISC)² CISSP CBK to support the European Cybersecurity Skills Framework / Cybersecurity professional communities

Introduction

The (ISC)² CISSP CBK – sometimes simply called the “Body of Knowledge” – refers to a peer-developed compendium of what a competent cybersecurity professional must identify and possess, including knowledge, skills, abilities, techniques and practices to be successful. The (ISC)² CBK is a collection of topics relevant to cybersecurity professionals around the world. It establishes a common framework of information security terms and principles which enables cybersecurity and IT/ICT professionals worldwide to discuss, debate and resolve matters pertaining to the profession with a common understanding, taxonomy and lexicon. (ISC)² was established, in part, to aggregate, standardize and maintain the (ISC)² CBK for cybersecurity professionals worldwide. The (ISC)2 CBK presents a readymade resource for current and aspiring cybersecurity professionals to adopt within the ECSF framework.

[29] https://www.isc2.org/-/media/9644E0ED44954F7CAF895D45620213EA.ashx

Challenge

As ENISA describes in their recently published report “Addressing The EU Cybersecurity Skills Shortage And Gap Through Higher Education”, global cybersecurity skills shortages and a lack of a sufficient and qualified workforce are concerns having a significant impact on EU member states ability to protect the public from increasing threats emanating from the ever-increasing use of technology in society. Despite work that has been accomplished, cyber-attacks and the threat of cyber-attacks continue to be a significant risk to public safety. European organizations are struggling to adequately staff their cybersecurity teams. The preventable consequences – misconfigured systems, rushed deployments, incomplete incident response, delayed patching, inadequate risk management – make many European organizations enticing targets for threat actors around the world.

Solution enabled by the ECSF (how the challenges were faced)

To meet the challenges presented by the skills gap and workforce shortage, (ISC)² proposes a solution focused on helping cybersecurity professionals identify and map needed knowledge, skills, abilities, techniques and practices to profiles identified in the European Cybersecurity Skills Framework (ECSF). The (ISC)2 CISSP CBK maps to several skills and knowledge areas in the following ECSF profiles:

- 2.1 Chief Information Security Officer (CISO)
- 2.2 Cyber Incident Responder
- 2.3 Cyber Legal, Policy & Compliance Officer
- 2.4 Cyber Threat Intelligence Specialist
- 2.5 Cybersecurity Architect
- 2.6 Cybersecurity Auditor

Using the concepts covered in the CBK, professionals who are currently working in the above listed profiles or those who are aspiring to work in these profiles can use the key skills and knowledge areas from the ECSF profiles combined with the (ISC)2 CBK to determine how the CBK fulfills the knowledge and skills required for the position and where they may need to supplement their education/training from other sources. This will enable candidates to build an educational/training path to achieve their goals.

The following table provides an example of how the (ISC)2 CISSP CBK can be used by a current or aspiring CISO to identify the key skills and knowledge areas from ECSF CISO Profile that they have or need to build. [...]

Result / Added value

The intended benefit of the (ISC)² CISSP CBK mapping to the ECSF is that it will create career guidance and professional educational pathways to assist current and aspiring cybersecurity professionals identify and obtain needed professional knowledge, skills and abilities in order to more rapidly obtain and fill open profiles, as identified in the ECSF, thereby mitigating global cybersecurity skills shortages and diminishing the qualified workforce gap.

B.6 USE CASE FROM ISACA

This section includes parts from the use case written by ISACA[30].

[30] https://www.isaca.org/training-and-events/careers-home/career-pathway/european-cybersecurity-skills-framework-and-isaca-credentials

Individual Career Decision Making: Professional Credentials European Cybersecurity Skills Framework

Introduction

Sabine was working as a SOC analyst a few years after obtaining her university degree, and was interested in learning how best to advance her career. She spoke with her mentor, who advised her that ISACA had been a great launching pad for his career and encouraged her to look into membership and eventual certification. One must realize that going into Cybersecurity gives the possibility to work with everything, from people and psychology via legal, policy, and governing, down to the lowest (or Highest) level technical level. The challenge is to find a starting point and then identify what specific competences one can learn and then master to broaden or even transition between cyber security roles. The ESCF specifies several roles with their competences needed to work within that specific role. Observe that these competences are not all that's needed for a specific role, but the bare minimum. By using this Sabine can identify the competence gap if one wants to change a role or move into another area within Cybersecurity.

Challenge

As a new professional in a high-demand field and as a woman in cybersecurity, Sabine was in seeking help in a few different areas:

- Career guidance and resources—including credentials—to help advance her career
- A network of peers and industry leaders to help her navigate professional challenges
- Assistance in developing soft skills to help her become well-rounded future leader
- Insights on overcoming challenges and leveraging opportunities as a woman in cybersecurity
- Information to help her do her current job well and help her prepare for future challenges in higher-level roles

Any individual can use the ESCF to see what roles are needed to handle almost any type of challenge or task within the cybersecurity domain. Also, by using the ESCF as a baseline an individual can then identify which competences are needed to move from one role to another. This will benefit the dialogue between employees and employers when planning the continuous education within the Cybersecurity field. This will also benefit an individual who wants to enter into Cybersecurity, but are unsure where to start. For most individuals adding to previous knowledge and competences is easier than learning something completely new.

With the mission of becoming a C-suite cybersecurity professional in this challenging field Sabine researched the outline of CISO responsibilities:

Profile 1 CISO Mission	Defines, maintains and communicates the cybersecurity vision, strategy, policies, and procedures and manages implementation across the organization. Governs cybersecurity related activities across the organization. Manages links/liaisons with external authorities and professional bodies.

Sabine's ambition is to identify the gaps in her skills in order to progress her career with an appropriately aligned credentials to the next level.

ECSF Solution

Sabine researched the ECSF PROFILE 1 and identified gaps in her knowledge:

Key knowledge	✓ Knowledge of cybersecurity and privacy standards, frameworks, policies, regulations, legislations, certifications and best practices Understanding of ethical cybersecurity organization requirements ✓ Knowledge of security controls Knowledge of cybersecurity maturity models ✓ Knowledge of cybersecurity tactics, techniques and procedures Knowledge of resource management Knowledge of management practices Knowledge of risk management frameworks

Sabine decided to take her mentor's advice and attend a local ISACA chapter meeting to see if it was the right fit. She was immediately impressed by the opportunities it provided. The chapter warmly welcomed her, introducing her to several key people in the chapter—people who worked in exactly the type of roles Sabine was seeking and would be excellent mentors or sponsors.

The chapter's certification chair informed Sabine that the Certified Information Security Manager (CISM) certification would be a great fit for her, as it demonstrates well-rounded knowledge of information security as well as strong managerial skills. The certification is for those with five or more years of experience, so Sabine decided to make an 18-month plan to study and obtain the certification.

She joined ISACA as a member that night and took full advantage of the resources the association offered at both the global and local levels. She joined the association's online communities, began attending webinars and local chapter meetings offered through SheLeadsTech, a program offered by ISACA's One in Tech Foundation. And she attended nearly every meeting the local chapter offered.

Just six months into her membership, a fellow chapter member approached her about a job as an information security analyst at their organization.

Result

Sabine has now been a member of ISACA for seven years. She earned her CISM certification and was soon promoted to information security manager. She is now a director of information security, with a clear path to a CISO role.

In addition to finding credentials and jobs through ISACA, Sabine also found several resources that helped her add value to her organization. Before GDPR went into effect, Sabine was able to leverage the GDPR Resource Hub offered by ISACA to help her understand the situation thoroughly and learn what the most critical steps to take were in her current role.

The interest and experience she gained in privacy as a result of that project enabled her to qualify for ISACA's Certified Data Privacy Solutions Engineer (CDPSE) credential through its early adopter program.

She has presented at ISACA conferences at the chapter and national levels—honing her communications skills—and she took on a chapter board position last year. As a director, she

has had the opportunity to hire for a few positions, and most of her hires have come from the ISACA chapter—just as she found her first promotion six years ago. Having seen the value of the CISM certification in her own career, she has begun offering CISM certification prep to her team through ISACA's enterprise training offerings.

Sabine's newest area of focus as she prepares for her CISO role is securing emerging technologies. Given the increased regulatory focus on AI in Europe, she has directed her efforts on that area first, recently obtaining an Artificial Intelligence Fundamentals Certificate from ISACA.

Seven years after walking through the doors of her first ISACA chapter meeting, Sabine has grown her network by hundreds of professionals locally and thousands globally. She is a

confident leader and speaker, and she is now a mentor to several others who were once in her position. Among her advice to her mentees is to always be learning—and that ISACA, as a global learning community, is a great resource.

Sabine has outlined steps to take to get the C-suite and plans to hold a CISO role within five years. She is confident that her ISACA network and credentials will be a significant advantage as she pursues her goals.

Career Path:

- SOC Analyst
- Information Security Analyst
- Information Security Manager
- Director of Information Security.

B.7 USE CASE FROM SANS/GIAC

This section includes parts from the use case written by SANS institute and GIAC (Global Information Assurance Certification)[31].

Why Workforce Frameworks and Certifications Matter in Cybersecurity

The Network and Information (NIS) II Directive is an update to the existing mandate for the European Union. This will help to encourage a common cyber security language across a broader range of sectors of the economy and will require sharing of information between member states and cross sectors. Directives like this one have increasing importance in establishing guardrails for cyber activities. To protect shareholder value, the Security and Exchange Commission (SEC) is considering a cyber report for publicly traded companies requiring reporting on how their security teams will manage risk, incidents, and the cyber expertise of the board of the directors. The security risk mitigation report will tie back to job roles skill sets.

Frameworks are helping to articulate these job roles. Most job openings until recently were generic listings seeking cyber security professionals without well-defined tasks, skills, or the knowledge of what is needed to protect the organizations assets. Workforce frameworks such as the ECSF European Cybersecurity Skills Framework (ECSF) are starting to standardize the talent needed for positions as a Cyber Incident Responder, Digital Forensics Investigator, and Chief Information Security Officer. Standardization enables organizations to identify the right

[31] https://www.giac.org/blog/why-workforce-frameworks-certifications-matter-cybersecurity/

talent to handle future threats. This is in-line with other professions. For example, doctors have specialized areas such as radiologists, pediatricians, and brain surgeons who have the expertise needed in their area to provide proper treatment.

Certification plays an important part in readying people for specific job roles. Certification validates the individual by utilizing best practices and guidelines for educational and psychological testing such as ISO/IEC 17024 International Standards. An example of a certification considered the global standard is a Certified Public Accountant (CPA). Work experience can make someone an expert, but the CPA is the well-respected baseline of a certified professional and can even be a requirement for compliance on specific projects or audits.

Some examples where workforce frameworks have helped advance the cyber security industry include:

- Large tech and financial firms often have multiple security teams that are standardizing their work roles and requirements through the framework to reposition and rotate workers quickly based on the mission.
- Organizations can map their workforce's experience and certification to quickly match staff skills with project requirements. This is especially important for consulting firms, tech firms, and contractors.
- Frameworks provide a common language in the workforce across industries like technology, financial, healthcare, retail, and utilities, allowing teams to work together to protect cyber and physical security threats.
- Frameworks provide a template for academic institutions to bridge the gap between their educational offerings and the current cyber security skills needed across industries, preparing their students for jobs.

SANS and GIAC understand the importance of frameworks and have aligned courses and certifications to these frameworks. Frameworks are a template for organizations to standardize job requirements even though every organization and mission will need some customization tied to their specific mission. We have helped design and implement workforce development programs using frameworks as a template for Fortune 500 companies, government agencies, and organizations of all sizes.

TP-09-22-509-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-583-8
DOI: 10.2824/95989