EUROPEAN
CYBERSECURITY
SKILLS FRAMEWORK

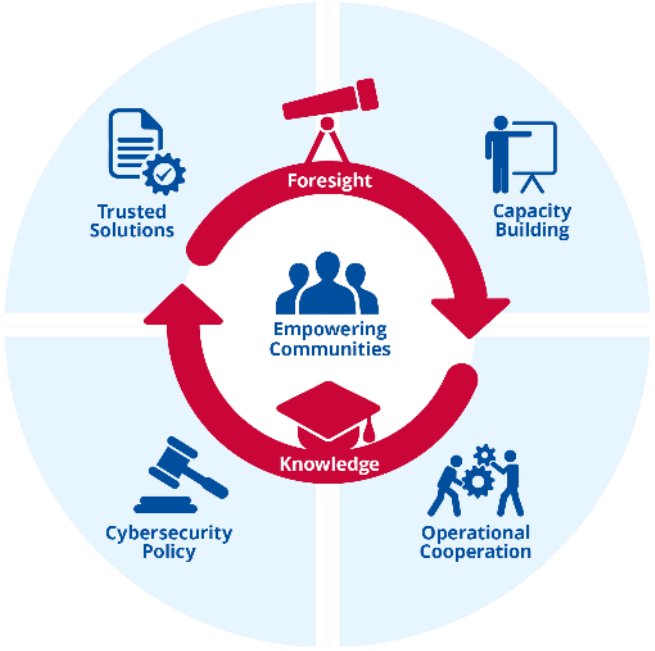
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

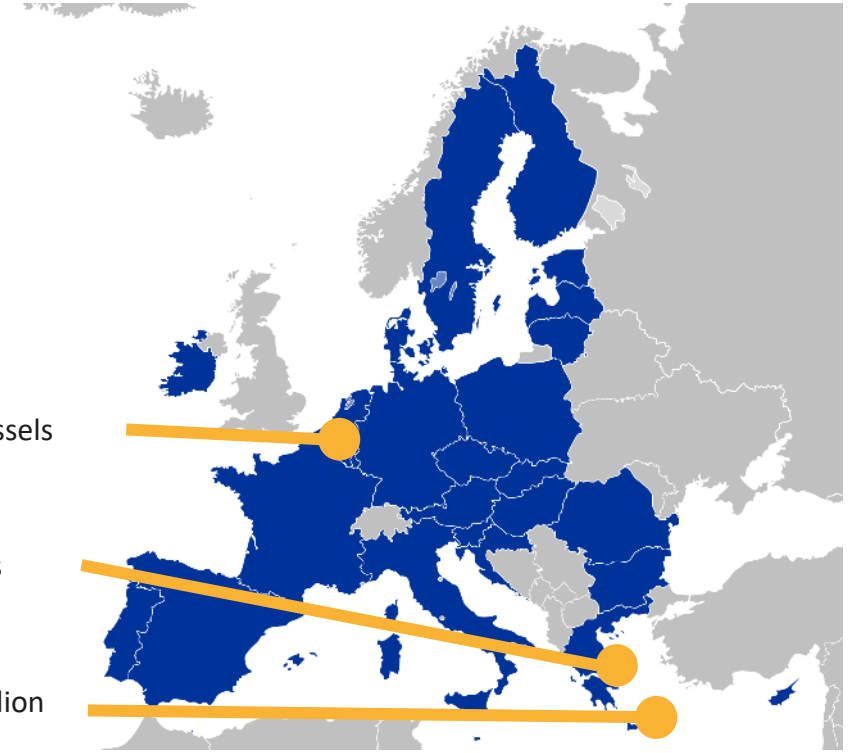
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

Evangelos Kantas
Anna Sarri
Awareness Raising and Education Team

19 06 2024

ABOUT ENISA





About 150 staff - steadily growing

4 units doing cybersecurity work

- Operational collaboration (Cyclone, CSIRT network)
- Cyber exercises, challenges, trainings (Cyber Europe)
- Certification and standardization (EU schemes)
- Policy unit (including EECC, eIDAS, NISD, 5G, eID wallets, critical sectors)

THE REVIEW OF THE ENISA FORESIGHT CYBER-SECURITY THREATS FOR 2030

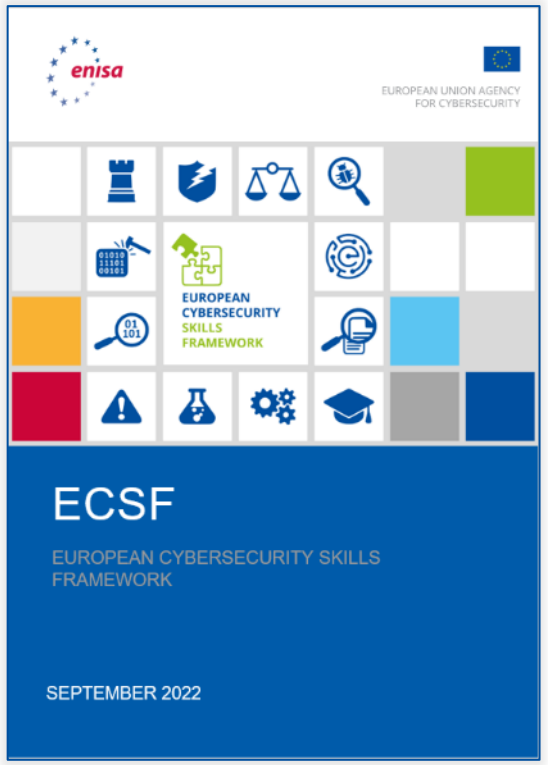
THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

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

Update info on the ECSF:
https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

ECSF COMPONENTS

The ECSF consists of 2 documents:

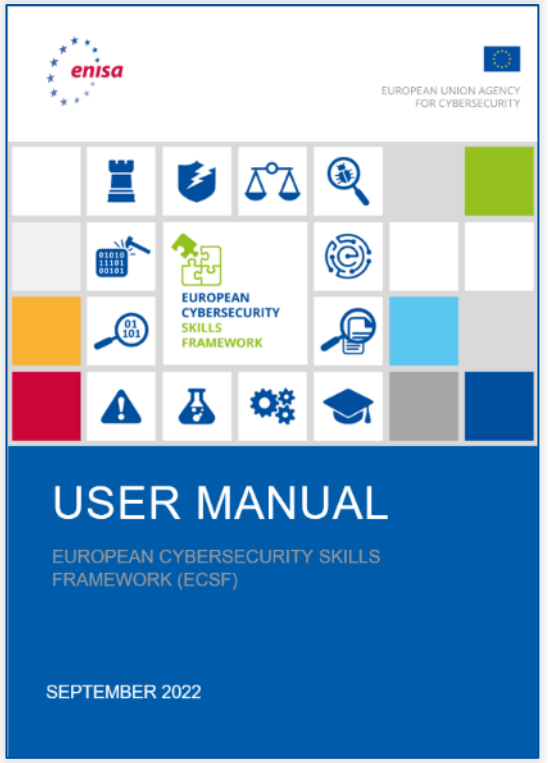


The ECSF Role Profiles

Listing the 12 typical cybersecurity professional role profiles along with their identified titles, missions, tasks, skills, knowledge, competences.

The ECSF User Manual

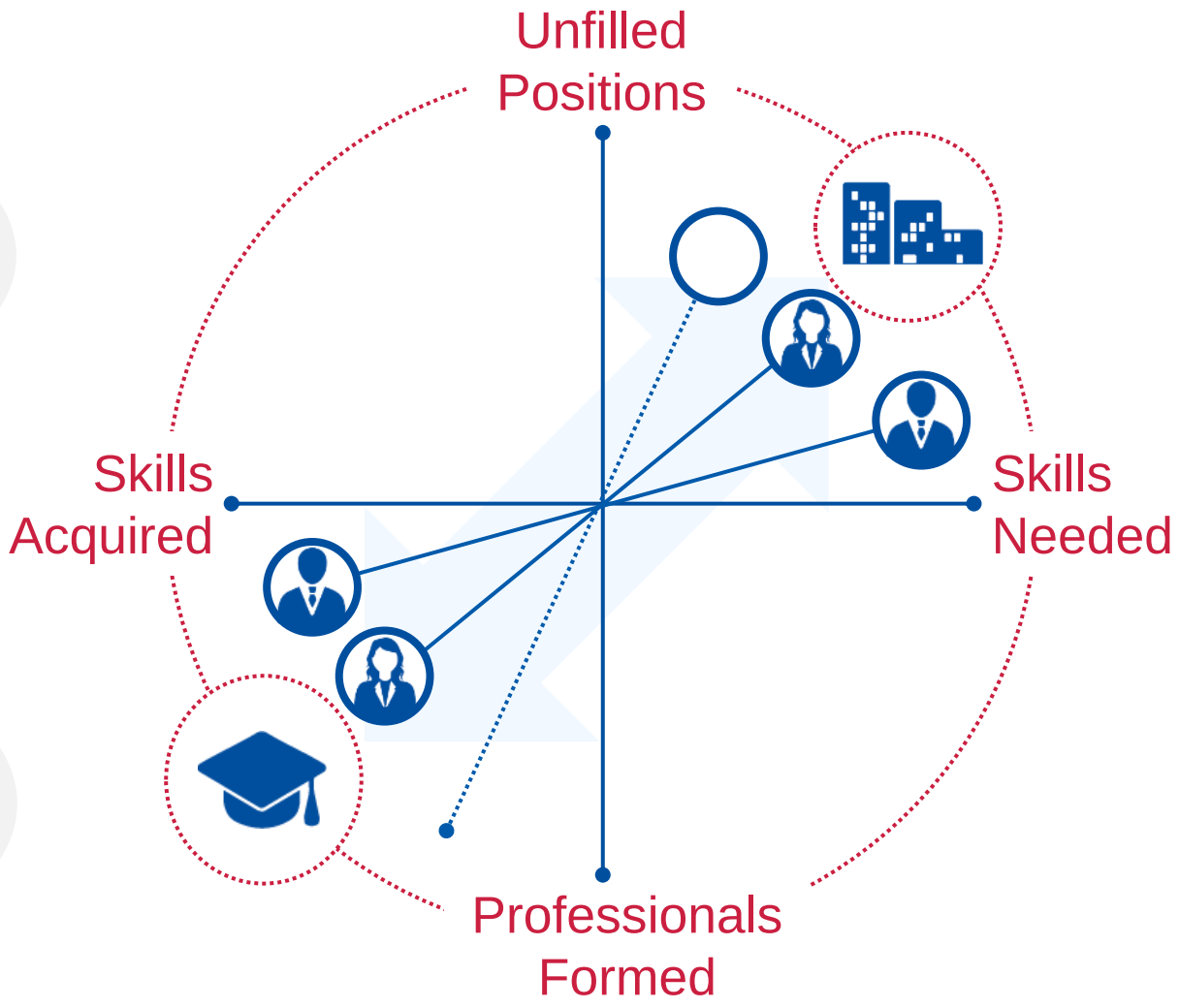
Providing guidance and practical examples on how to leverage the framework and benefit from it as an organisation, provider of learning programmes, or individual.



CYBERSECURITY SKILLS GAP - CHALLENGES

Which skills must professionals acquire?

How big is the workforce shortage?



How many professionals are joining the workforce?

Which skills are needed in the workforce?

THE ECSF OBJECTIVES

The ECSF aims to:

- Create a **common understanding** of the necessary roles, competencies, skills and knowledge
- Facilitate **cybersecurity skills recognition**
- Support the **design of** cybersecurity-related **training programs**

BENEFITS IN USING ECSF

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

We are looking for a Risk Manager!

Organisations

Which skills our candidates should have?

We are training Risk Managers!

Learning providers

What should be included in our training offers?

I want to became a Risk Manager!

Individuals

Which skills and knowledge do I need?

enisa

THE 12 CYBERSECURITY PROFILES

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

- Chief Information Security Officer (CISO)
- Cyber Incident Responder
- Cyber Legal, Policy and Compliance Officer
- Cyber Threat Intelligence Specialist
- Cybersecurity Architect
- Cybersecurity Auditor
- Cybersecurity Educator
- Cybersecurity Implementer
- Cybersecurity Researcher
- Cybersecurity Risk Manager
- Digital Forensics Investigator
- Penetration Tester

enisa

CORE CYBERSECURITY FUNCTIONS & DELIVERABLES

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Chief Information Security Officer (CISO)	Cybersecurity Governance, Strategy & policies
Cybersecurity Risk Manager	Cybersecurity Risk Assessment & Remediation Action Plan
Cybersecurity Architect	Architecture Diagram & Requirements
Cyber Incident Responder	Monitoring, Incident planning & Incident Report
Cybersecurity Educator	Cybersecurity Awareness Program

enisa

PROFILE OVERVIEW: CHIEF INFORMATION SECURITY OFFICER (CISO)

Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.

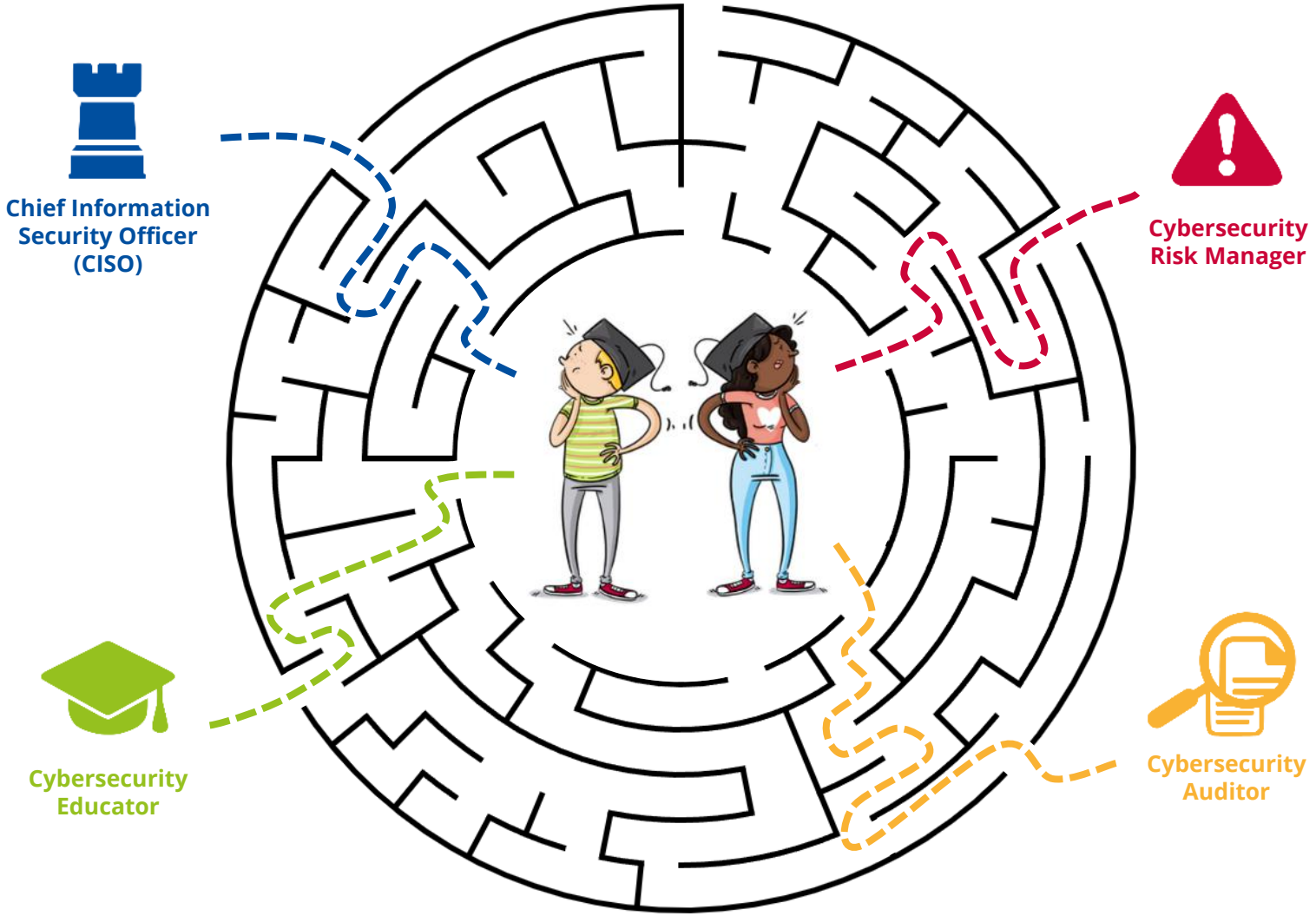
- Cybersecurity Strategy
- Cybersecurity Policy

EXAMPLE

Profile Title	Chief Information Security Officer (CISO)
Alternative Title(s)	Cybersecurity Programme Director Information Security Officer (ISO) Information Security Manager Head of Information Security IT/ICT Security Officer
Summary statement	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.
Mission	Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.
Deliverable(s)	• Cybersecurity Strategy • Cybersecurity Policy
Main task(s)	• Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives • Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution • Supervise the application and improvement of the Information Security Management System (ISMS) • Educate senior management about cybersecurity risks, threats and their impact to the organisation • Ensure the senior management approves the cybersecurity risks of the organisation • Develop cybersecurity plans • Develop relationships with cybersecurity-related authorities and communities • Report cybersecurity incidents, risks, findings to the senior management • Monitor advancement in cybersecurity • Secure resources to implement the cybersecurity strategy • Negotiate the cybersecurity budget with the senior management • Ensure the organisation's resiliency to cyber incidents • Manage continuous capacity building within the organisation • Review, plan and allocate appropriate cybersecurity resources

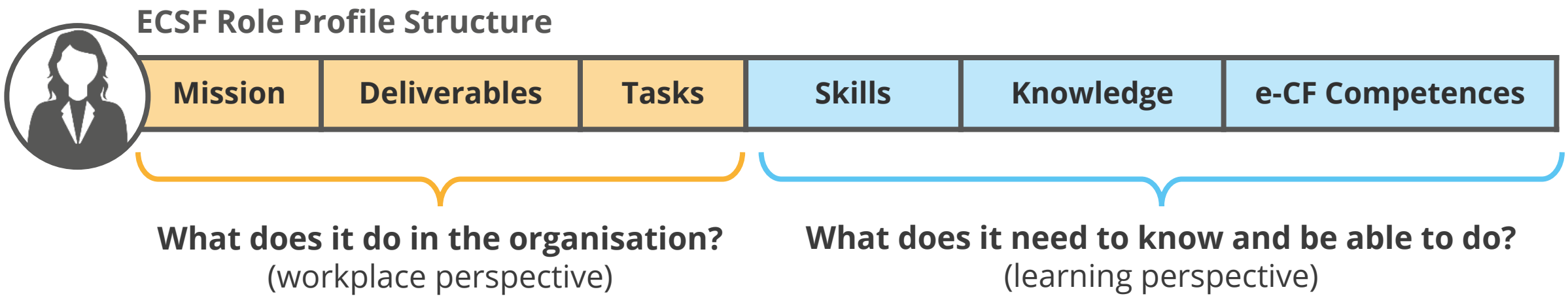
Key skill(s)	• Assess and enhance an organisation's cybersecurity posture • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Analyse and comply with cybersecurity-related laws, regulations and legislations • Implement cybersecurity recommendations and best practices • Manage cybersecurity resources • Develop, champion and lead the execution of a cybersecurity strategy • Influence an organisation's cybersecurity culture • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Review and enhance security documents, reports, SLAs and ensure the security objectives • Identify and solve cybersecurity-related issues • Establish a cybersecurity plan • Communicate, coordinate and cooperate with internal and external stakeholders • Anticipate required changes to the organisation's information security strategy and formulate new plans • Define and apply maturity models for cybersecurity management • Anticipate cybersecurity threats, needs and upcoming challenges • Motivate and encourage people	
Key knowledge	• Cybersecurity policies • Cybersecurity standards, methodologies and frameworks • Cybersecurity recommendations and best practices • Cybersecurity related laws, regulations and legislations • Cybersecurity-related certifications • Ethical cybersecurity organisation requirements • Cybersecurity maturity models • Cybersecurity procedures • Resource management • Management practices • Risk management standards, methodologies and frameworks	
e-Competences (from e-CF)	A.7. Technology Trend Monitoring D.1. Information Security Strategy Development E.3. Risk Management E.8. Information Security Management E.9. IS-Governance	Level 4 Level 5 Level 4 Level 4 Level 5

The ECSF Links Employment with Education



Bridging Market & Education

ECSF profiles are structured in a way that links educations with the requirements of the job market.



EXAMPLE

ENHANCING THE CYBERSECURITY PRACTICES OF A SMALL COMPANY

The founders of a

Cloud Services Company

used

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

identified that their organisation

required five key roles to support their cybersecurity baseline

- 1× Strategic Cybersecurity Manager (CISO)
- 1× Cybersecurity Legal Officer
- 1× Cybersecurity Architect
- 3× Cybersecurity Implementers
- 1× Cyber Incident Responder

EXAMPLE

ENHANCING THE CYBERSECURITY PRACTICES OF A SMALL COMPANY

Cyber Legal, Policy and Compliance Officer	1×	**Cybersecurity Legal Officer**	**Train Legal Officer**
Cybersecurity Architect	1×	**Cybersecurity Architect**	**Train ICT Architect**
Cybersecurity Implementer	3×	**Cybersecurity Implementers**	**Train ICT Specialists**
Chief Information Security Officer (CISO)	1×	**Strategic Cybersecurity Manager (CISO)**	**Recruit a Strategic Cybersecurity Manager**
Cyber Incident Responder	1×	**Cyber Incident Responder**	**Outsource Incident Response**

upskilling employees

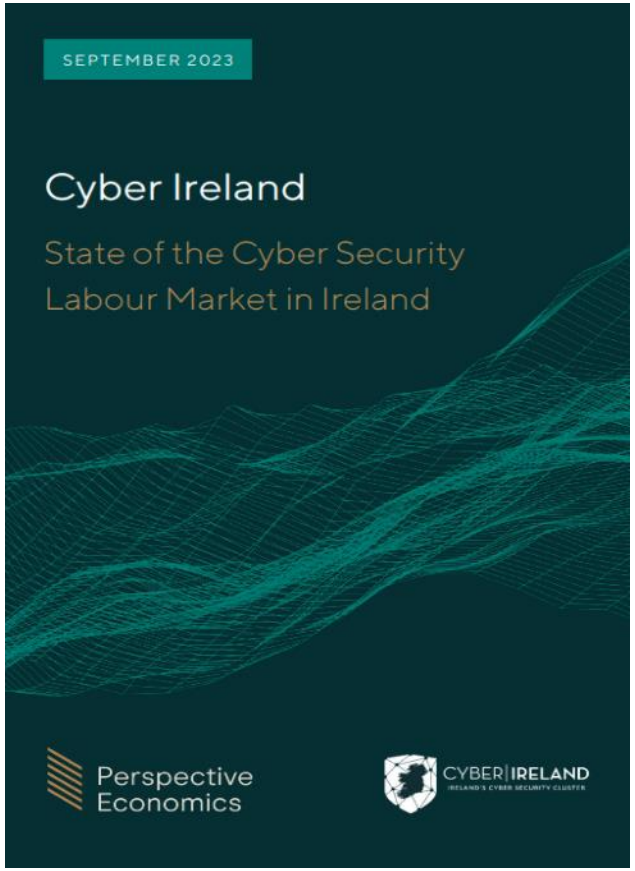
recruiting personnel

collaborate with externals

EXAMPLE

ENHANCING THE CYBERSECURITY PRACTICES OF A SMALL COMPANY

WHAT KIND OF SKILLS?



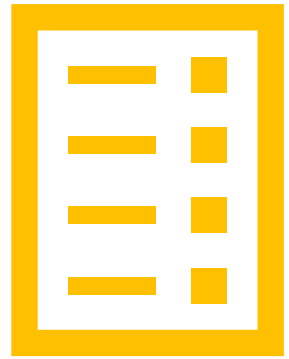
Cybersecurity Implementer	46%
Cyber Incident Responder	13%
Cybersecurity Risk Manager	12%
Chief Information Security Officer (CISO)	8%

ISC2 WORKFORCE STUDY 2023

In which of the following areas/roles is your organization lacking cybersecurity talent?

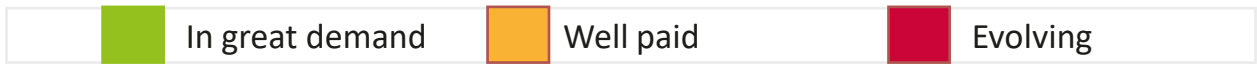
Cybersecurity Architect	30%
Cybersecurity Implementer	25%
Cyber Incident Responder	25%
Digital Forensics Investigator	24%

Survey: >2,000 respondents in the EU



HOW IT LOOKS TODAY

- Chief Information Security Officer (CISO)
- Cyber Incident Responder
- Cyber Legal, Policy & Compliance Officer
- Cyber Threat Intelligence Specialist
- Cybersecurity Auditor
- Cybersecurity Researcher
- Digital Forensics Investigator
- Penetration Tester
- Cybersecurity Architect



TOWARDS COMPLIANCE

NIS2	Cyber Solidarity Act	Managed Secure Service Providers
• **Chief Information Security Officer** • Cyber Incident Responder • Cybersecurity Risk Manager • Cyber Legal, Policy & Compliance Officer • **Penetration Tester**	• Cyber Incident Responder • Penetration Tester • Cybersecurity Risk Manager	• Cyber Incident Responder • Penetration Tester • Cybersecurity Auditor • Chief Information Security Officer

Common skills needs across the legal requirements…

ECSF ADOPTED BY COMMUNITIES

IMPLEMENTATION BY MEMBER STATES

Portugal: National skills framework mapped to ECSF

Cyprus: The Digital Security Authority (DSA) has adopted the ECSF for their internal positions. Also considering adoption for public roles and the CISO profile in the critical sectors.

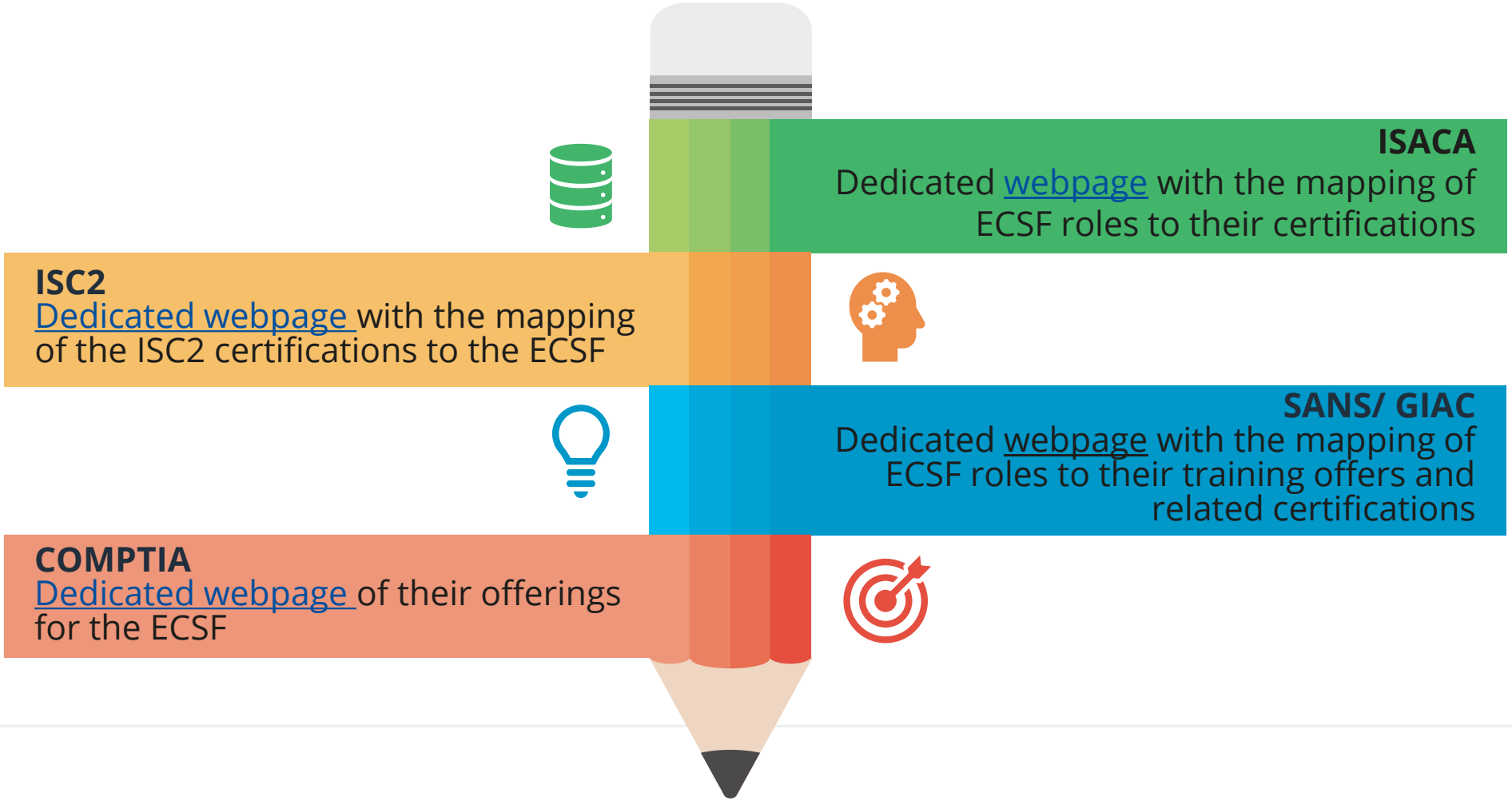
Spain: INCIBE is promoting the ECSF as a national standard in the National Cybersecurity Forum (a PPP with representation from Industry, Academia, Administration) in order to standardize employment needs and develop capacity building activities aligned to it.

Italy: Cybersecurity Agency is developing vocational training courses aligned to the ECSF

Poland: Cybersecurity Skills Council has adopted the ECSF and is adapting to the Polish context

Survey results:
20 MSs agree on the ECSF as a common taxonomy

CERTIFICATIONS MAPPING



ISACA
Dedicated webpage with the mapping of ECSF roles to their certifications

ISC2
Dedicated webpage with the mapping of the ISC2 certifications to the ECSF

SANS/ GIAC
Dedicated webpage with the mapping of ECSF roles to their training offers and related certifications

COMPTIA
Dedicated webpage of their offerings for the ECSF

CYBERSECURITY SKILLS ACADEMY

Increase the number of cybersecurity professionals, including the share of women in the field

Reduce the gap between the offer and demand of cybersecurity skills on the labour market

Provide the skills needed to meet cybersecurity legal and policy requirements at EU or national level

Equip citizens with in-demand cybersecurity skills

Improve the visibility and synergies between public and private initiatives on cybersecurity skills

Improve comparability, quality assurance, and certification of cybersecurity skills

https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

INDICATORS

Cybersecurity professional / specialist

A cybersecurity professional is an individual who occupies a position associated to a role profile described in the European Cybersecurity Skills Framework (ECSF).

These professionals are responsible for safeguarding computer systems, networks, and data from various forms of cyber threats, including cyberattacks, data breaches, malware, and other security risks. They play a crucial role in protecting digital assets, ensuring data confidentiality, integrity, and availability, and responding to and mitigating cybersecurity incidents.

Indicator: (1) No of professionals, (2) %of Women

SOURCE: NCCs /Eurostat

Cybersecurity graduates

A cybersecurity graduate is an individual who has successfully completed a formal higher education programme on cybersecurity. This formal education typically leads to the attainment of a degree in a cybersecurity-related field at **qualification level 6 or 7 according to the European Qualification Framework (EQF)** Cybersecurity graduates have advanced or high specialised acquired knowledge, skills, and expertise in various aspects of cybersecurity, and they are prepared to apply these skills in professional settings to address cybersecurity challenges and protect digital assets. Cybersecurity graduates play a vital role in addressing the growing demand for skilled cybersecurity professionals.

Indicator: (1) No of graduates, (2) % of Women

SOURCE: CyberHEAD

CYBERHEAD

the largest updated hub for students seeking a cybersecurity university programme

146 cybersecurity programmes
(from 125 programme in 2022)

Provide trends for graduates & their gender balance.

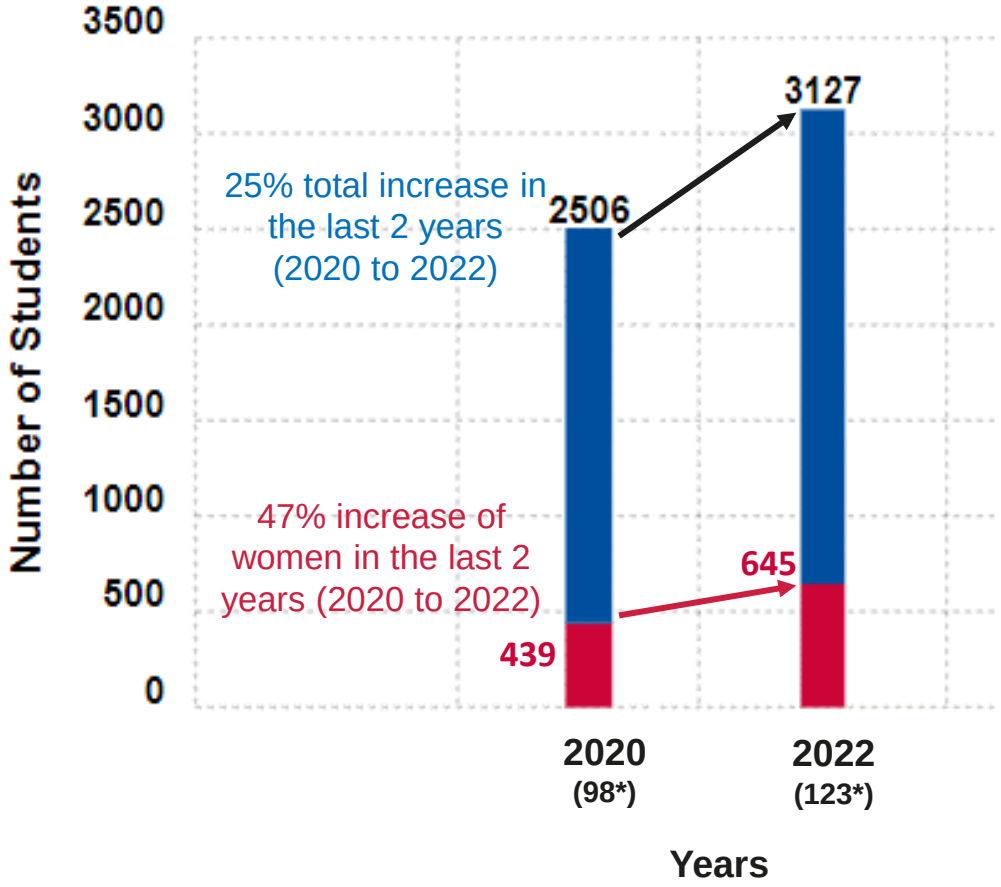
ECSF mapping
(skills acquired)

Supply side of the skills gap and shortage: how many graduates are available (to join the workforce) and their skillset.

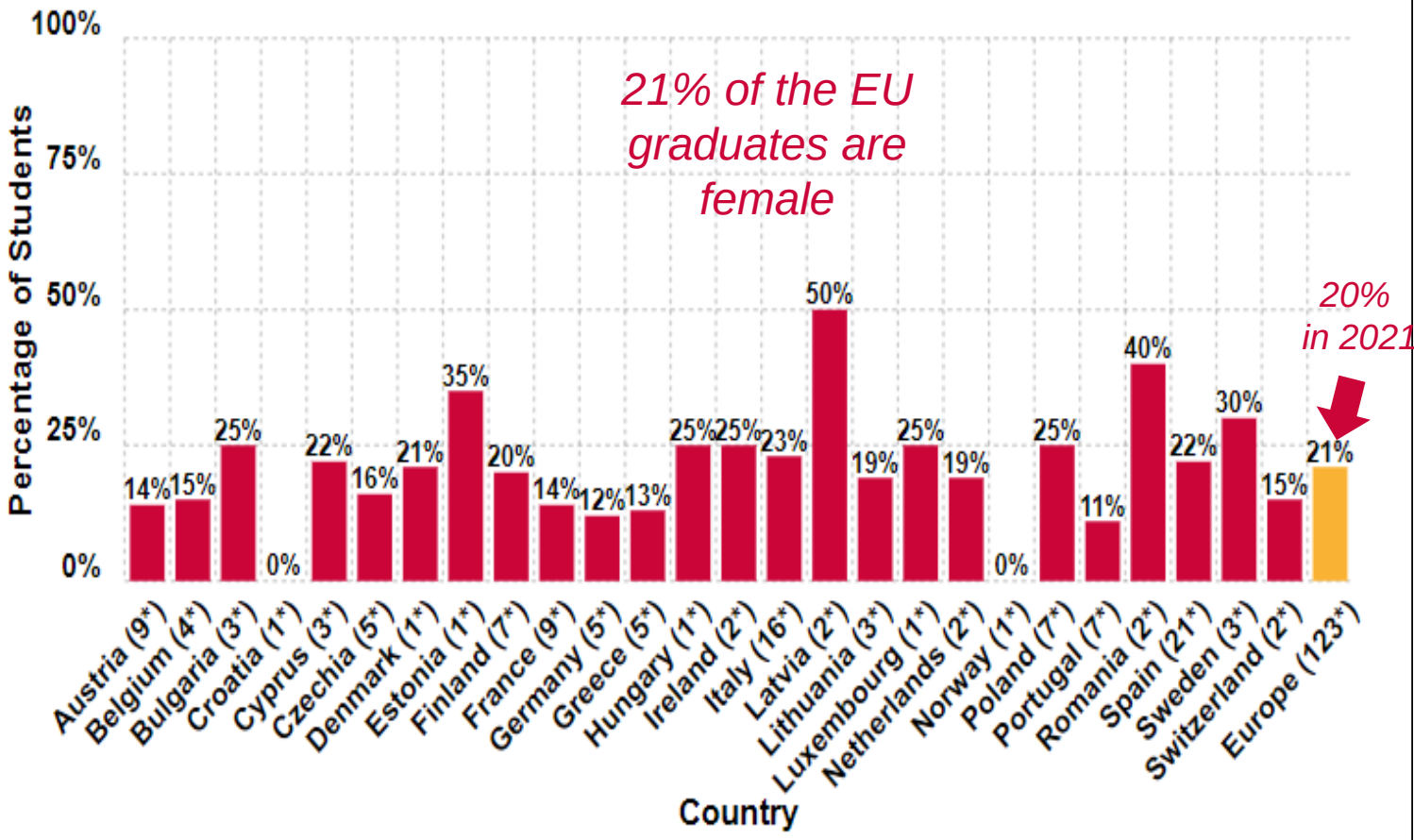
SOME INSIGHTS FROM THE SUPPLY SIDE

CYBERSECURITY HIGHER EDUCATION DATABASE
CYBERHEAD

COMPARISON BETWEEN 2020 AND 2022 GRADUATES



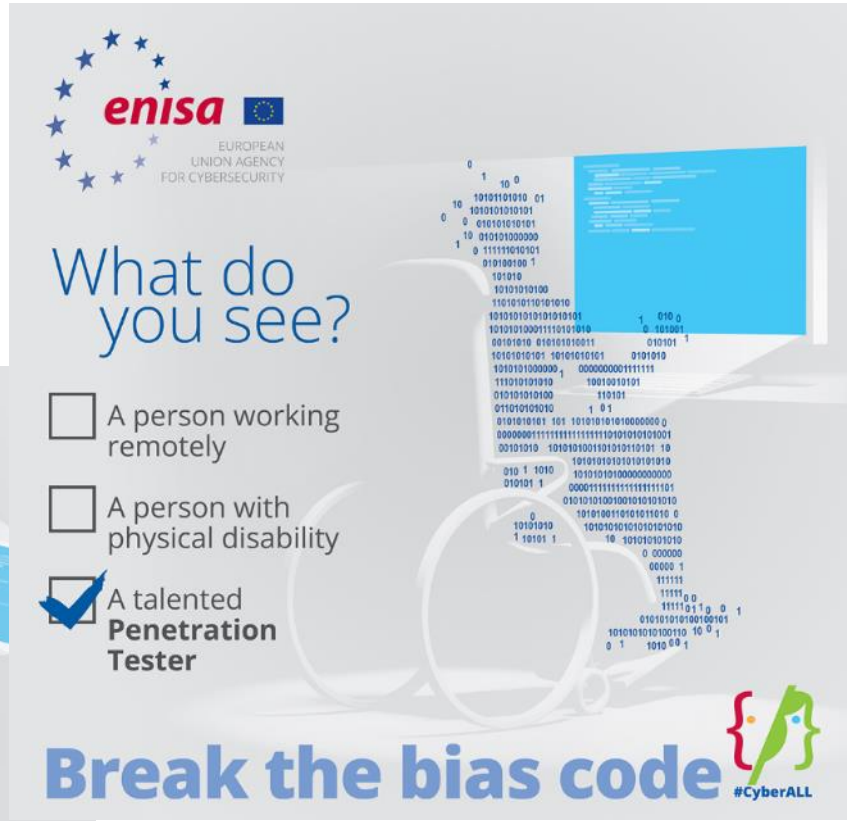
FEMALE PERCENTAGE OF GRADUATES IN 2022



Full report available here

enisa

EXPANDING THE TALENT POOL – CYBERALL CAMPAIGN



THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

+111 123 456 789

info@enisa.europa.eu

www.enisa.europa.eu