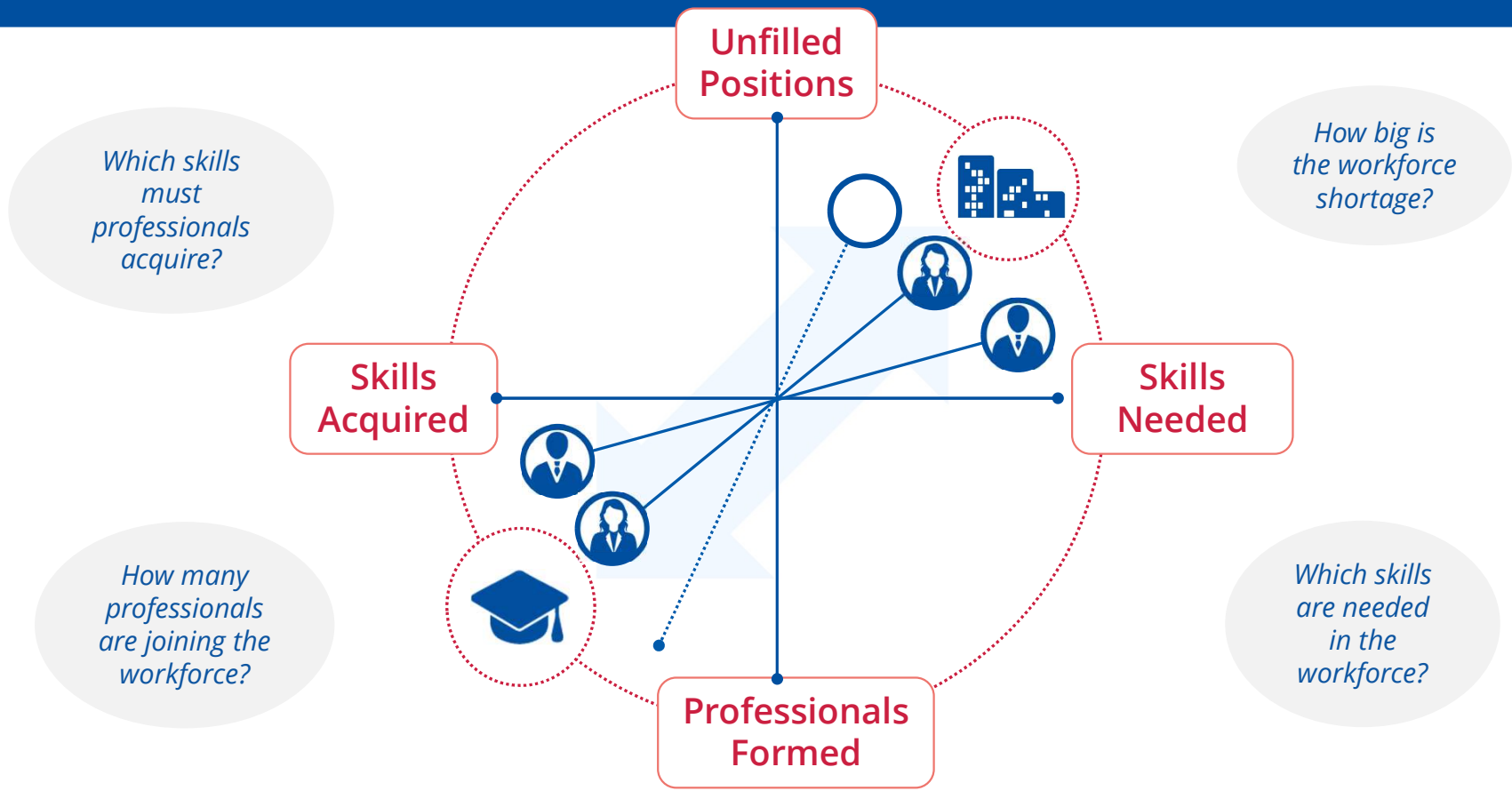
ETSI Security Conference 2025

The European Cybersecurity Skills Framework (ECSF)

Sławomir Górniak / Fabio i Franco

09/10/2025

Cybersecurity Skills Gap & Shortage in Europe



The European Cybersecurity Skills Framework (ECSF)

The ECSF provides an open tool to build

- ✓ a **common understanding** of the cybersecurity professional role profiles in **Europe** &
- ✓ **common mappings** with the appropriate skills and competences required.

The ECSF was designed to be

- ✓ **Simple yet Comprehensive**
- ✓ **Flexible & Scalable**
- ✓ **Open & Impartial**

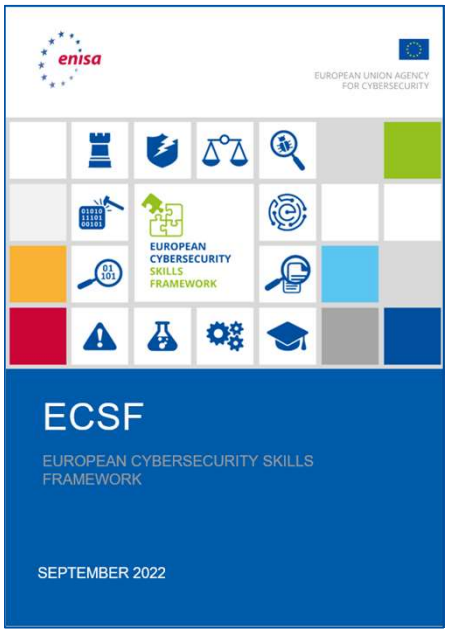
The ECSF

- Provide a **common understanding** of typical professional work roles and tasks, with competences, skills and knowledge required
- Facilitate **cybersecurity professional skills recognition**
- Support **cybersecurity workforce planning and development**
- Support the **design of** cybersecurity-related **training programmes**

Updated info on the ECSF:
European Cybersecurity Skills Framework (ECSF) | ENISA

EUROPEAN
CYBERSECURITY
SKILLS FRAMEWORK

ECSF Components

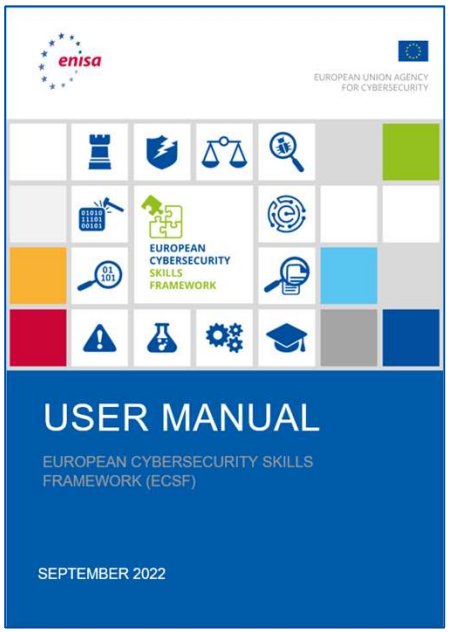


The ECSF Role Profiles

Listing the 12 typical cybersecurity professional role profiles along with their identified main title, alternative titles, mission, 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.



The 12 Cybersecurity Role Profiles

Chief Information Security Officer (CISO)

Cyber Incident Responder

Cyber Legal, Policy and Compliance Officer

Cyber Threat Intelligence Specialist

Cybersecurity Architect

Cybersecurity Auditor

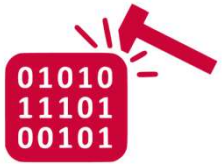
Cybersecurity Educator

Cybersecurity Implementer

Cybersecurity Researcher

Cybersecurity Risk Manager

Digital Forensics Investigator



Penetration Tester

Chief Information Security Officer (CISO)

example

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

Role Profile — Full description

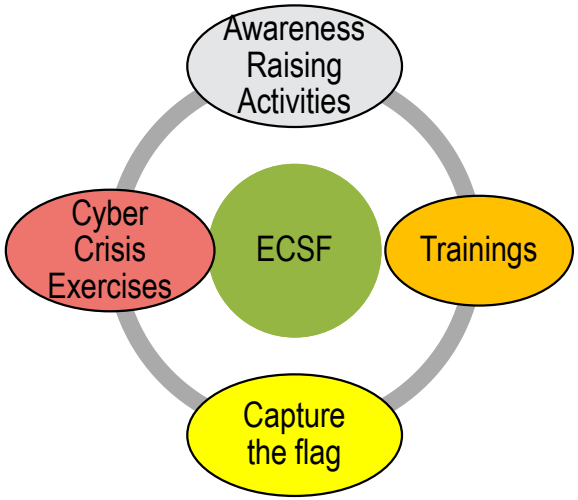
example

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

How the ECSF is used

Capacity building



Who is using the ECSF and Why

1. Education & Training Providers

- Align curricula with ECSF roles
- Develop targeted upskilling/reskilling programs

2. Employers & Industry

- Standardize job descriptions
- Identify internal skill gaps & plan workforce development

3. Policymakers & Authorities

- Build national skills strategies
- Benchmark and report on shortages to guide funding

4. Professional Associations

- Map certifications to ECSF competencies
- Develop assessment tools and common terminology

5. EU Projects & Research

- Integrate ECSF into project deliverables
- Create tools to facilitate the ECSF implementation

ECSF Impact at institutional level

17 EU Member States are using the ECSF

How ?

- National standard (few MSs)
- Cybersecurity training paths
- Public sector recruitment
- Workforce assessment taxonomy

ECSF is defined as the reference framework for cybersecurity skills in the EU in the European Commission Communication on the Cyber Skill Academy

Feasibility study on the attestation of skills

To further address the cybersecurity talent gap, ENISA is leading a **feasibility study** a **European attestation scheme** for cybersecurity skills. The goal is to:

- Define **scenarios for skill validation** linked to ECSF role profiles
- Promote **cross-border recognition** and **portability of skills**
- Facilitate **recruitment and mobility** for both employers and professionals.

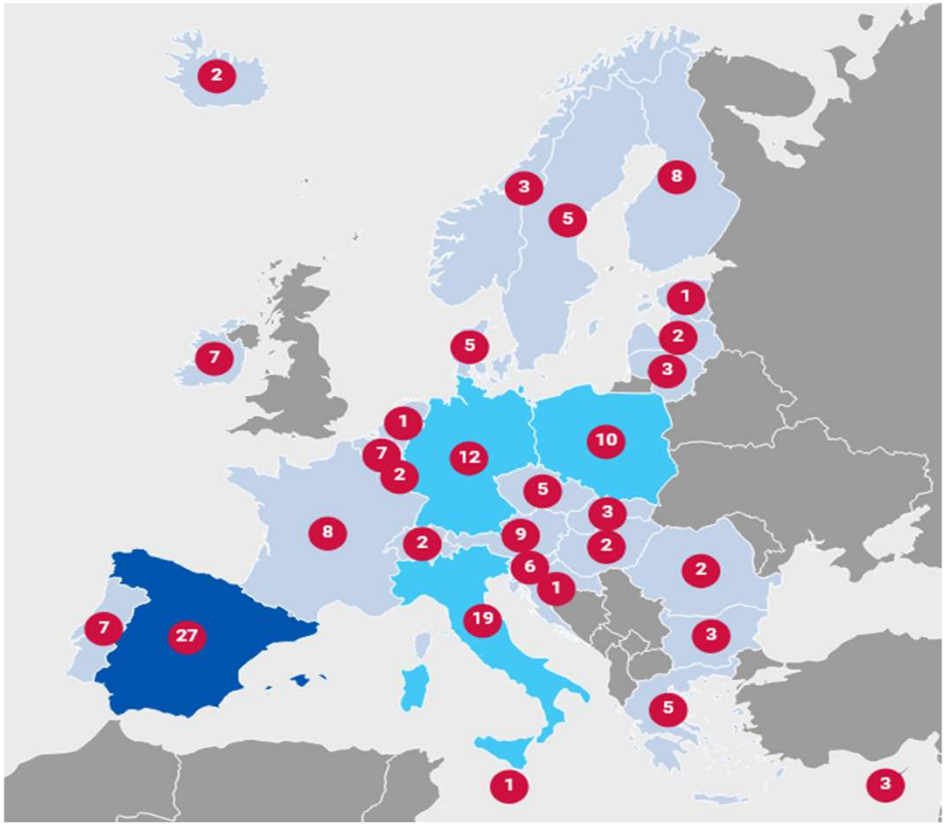
Seven Member States have joined the feasibility study. **Results are expected in Dec 2025**

Cyber in academia: CyberHEAD

The most comprehensive and up-to-date reference point for prospective students to explore and select the **academic programme** in cybersecurity

170+ cybersecurity programmes in the EU and EFTA countries

Linked to the ECSF to help students understand the possible career paths



https://www.enisa.europa.eu/CyberHEAD

ECSF is a global reference for capacity building

International Certifications

CompTIA

ISACA

ISC2

SANS GIAC CERTIFICATIONS

CREST

EC-Council
Building A Culture Of Security

Tools

Road 2 Cyber
Powered by ECSO and Women4Cyber

CyberHubs

Eu Capacity building projects

REWIRE
Cybersecurity Skills Alliance

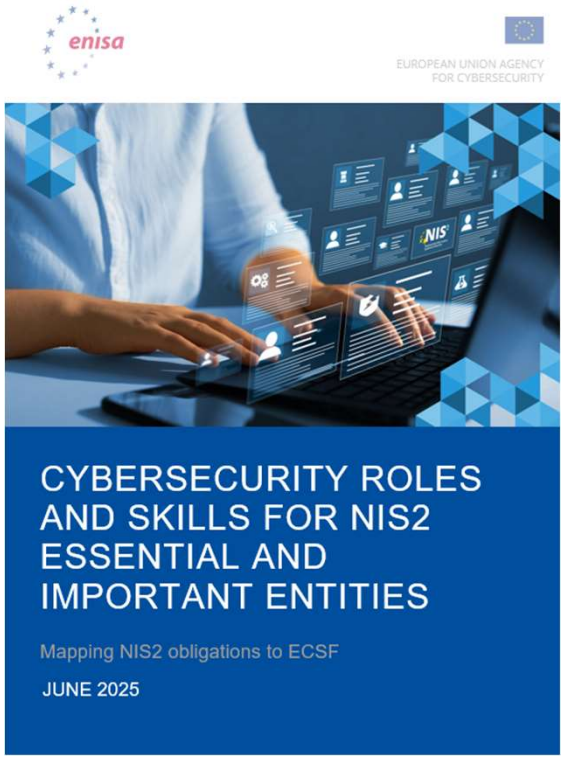
CyberSecPro

NERO
advaNced cybErsecurity
awaReness ecOsystem for SMEs

CYBER SYNCHRONY

And many more….

ECSF helps NIS2 implementation



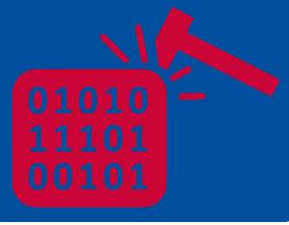
- NIS2 obligations mapped to ECSF roles: helps entities and national authorities translate legal obligations into concrete workforce capabilities
- 2 use cases help medium-sized organisations to build required cybersecurity capabilities

ECSF applied to the AI: methodology

- **Legal aspect** – defining the cybersecurity legal and regulatory needs of a specific sector/domain
- **Security aspect** – analysing the various sectors or domain-specific assets that need to be protected
- **Risk aspect** – covering the specific types of risks associated with the analysed domain
- **Tools aspect** – ensuring the inclusion of tools used in the sector/domain in question
- **Threat aspect** – considering sector or domain-specific threats and threat actors

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

ECSF applied to the AI: contextualization



Penetration Tester

	ECSF Penetration Tester		Penetration Tester specialising in AI
Summary Statement	Assesses the effectiveness of security controls, reveals and utilises cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors.	→	Assesses the effectiveness of security controls ***protecting AI-related systems***, reveals and utilises cybersecurity ***AI-related* vulnerabilities**, assessing their criticality if exploited by threat actors ***and uses AI-enabled tools or methodologies for penetration testing engagements***.
Skill	Perform social engineering	→	Perform social engineering *using* ***generative AI***
Knowledge	Cybersecurity recommendations and best practices	→	***AI-related systems security and trustworthiness*** recommendations and best practices

Thank you!

EuSkills@enisa.europa.eu

www.enisa.europa.eu