



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

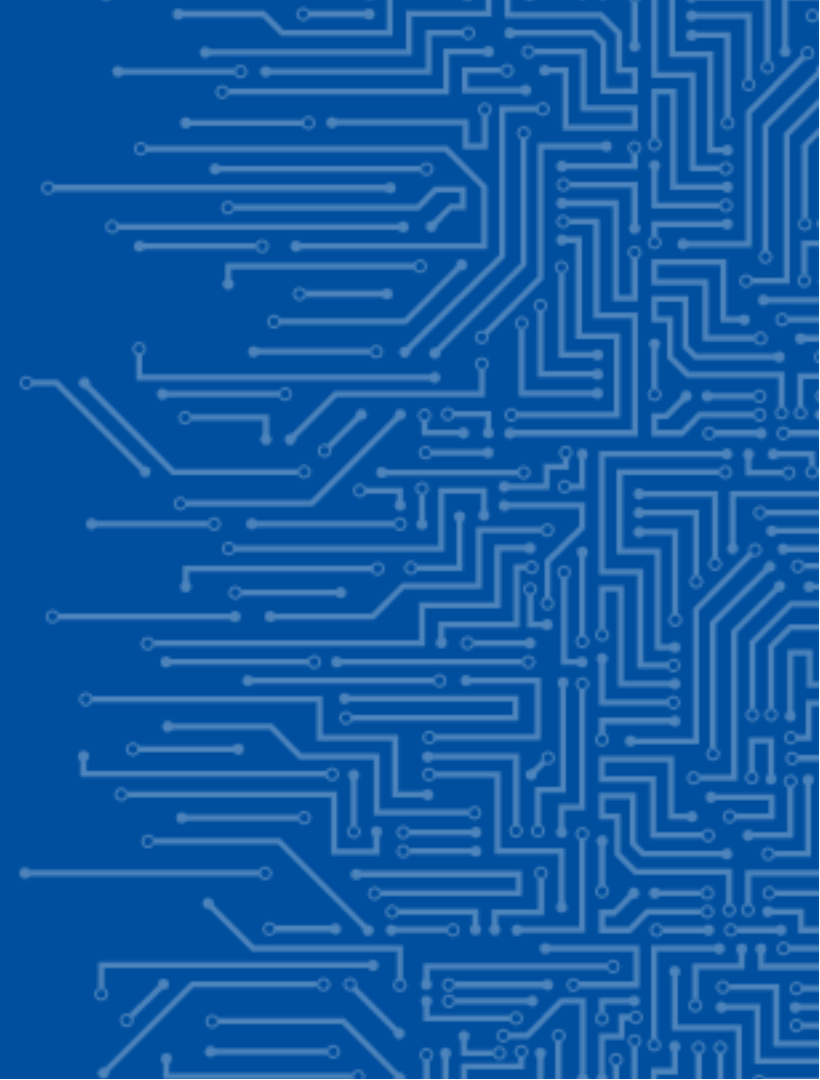


EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

... IN THE RAILWAY SECTOR

Dr. Fabio Di Franco

08 | 11 | 2023



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**



EXAMPLE: CHIEF INFORMATION SECURITY OFFICER (CISO)



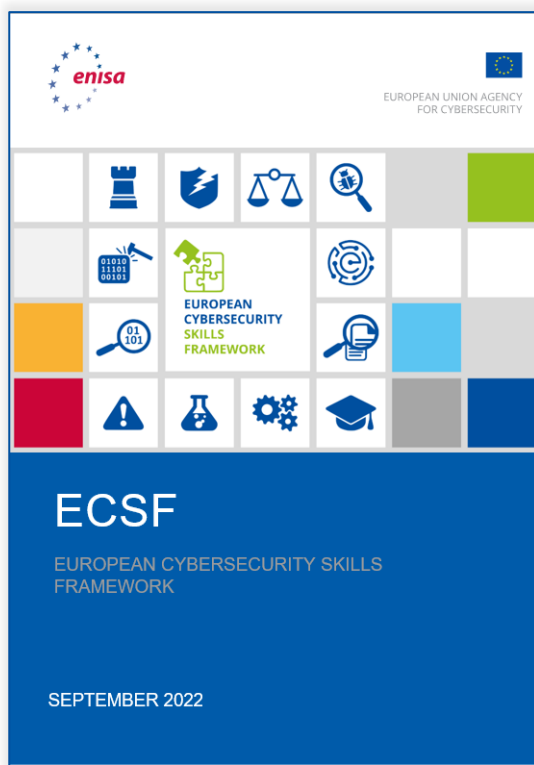
Profile Title	Chief Information Security Officer (CISO)
Alternative Title(s)	Cybersecurity Programme Director Information Security Officer (ISO) Information Security Manager Head of Information Security IT/ICT Security Officer
Summary statement	Manages an organisation's cybersecurity strategy and its 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)	<ul style="list-style-type: none"> • Cybersecurity Strategy • Cybersecurity Policy
Main task(s)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)



The framework consists of 2 documents:

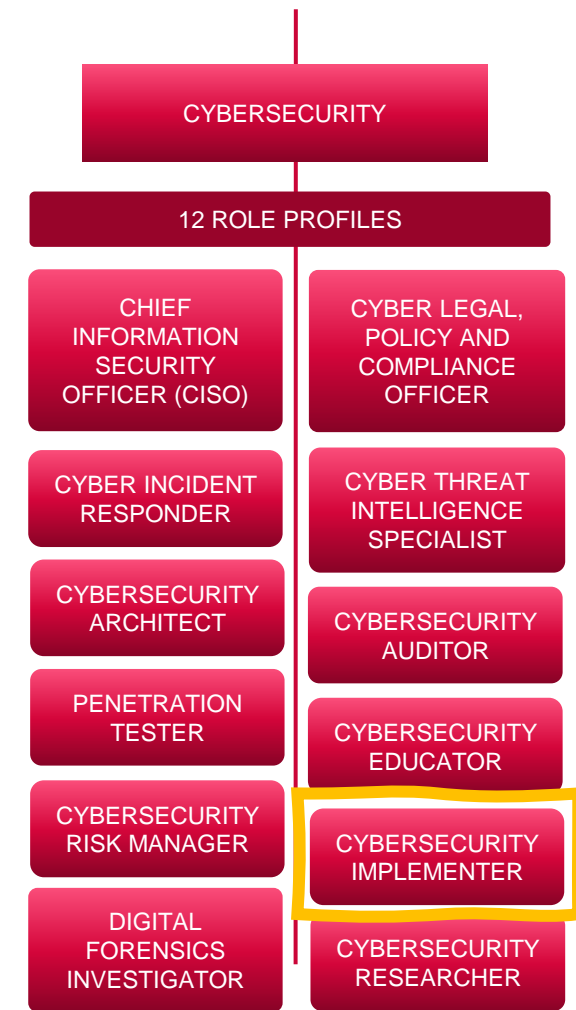
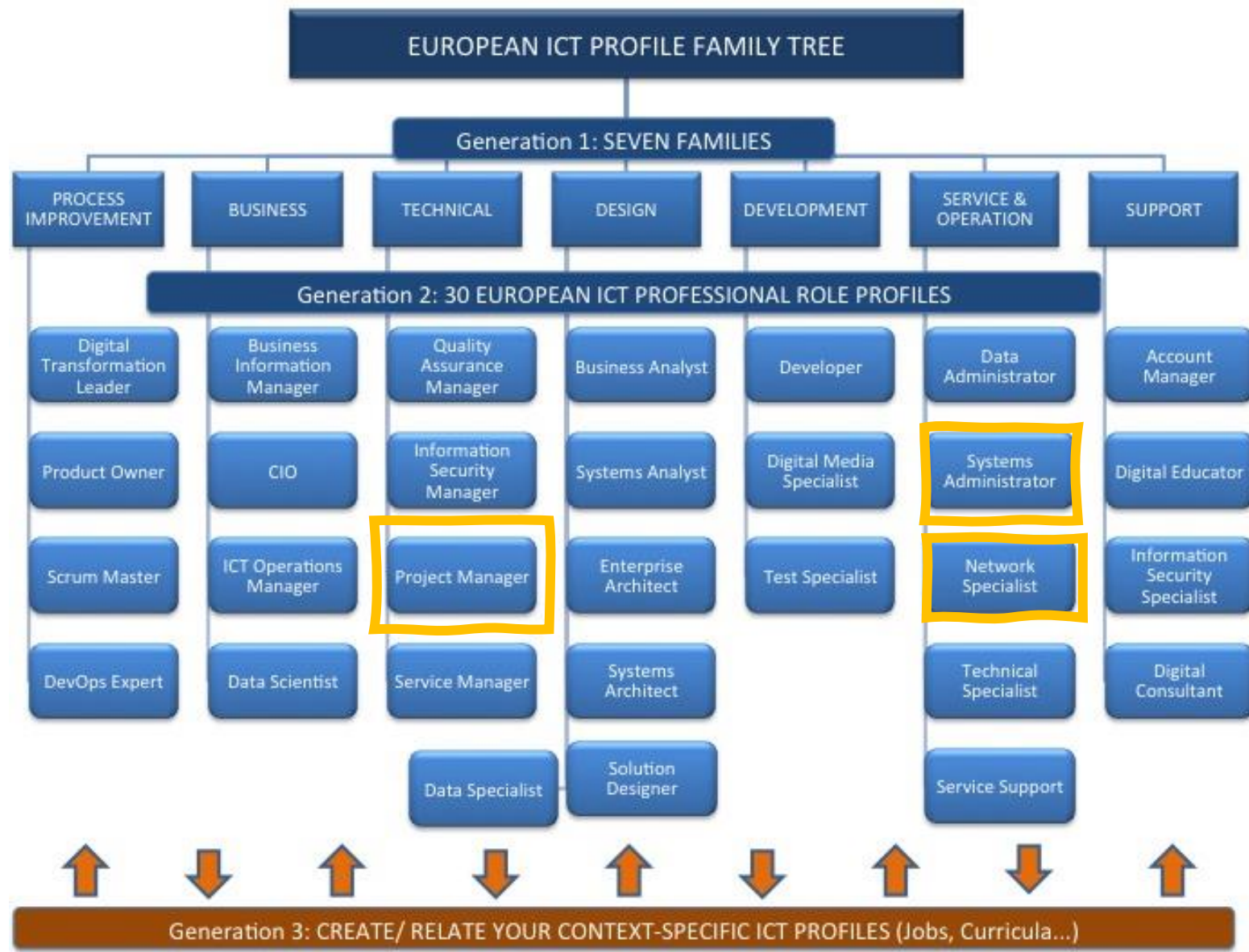


The ECSF Role Profiles document
Listing the 12 typical cybersecurity professional role profiles along with their identified titles, missions, tasks, skills, knowledge, competences.



The ECSF User Manual document
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 & ICT PROFESSIONAL FRAMEWORKS



<https://itprofessionalism.org/about-it-professionalism/competences/ict-profiles/>

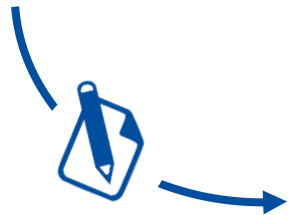


IEC 63452 DRAFT

RAILWAY APPLICATIONS – CYBERSECURITY



EUROPEAN
CYBERSECURITY
SKILLS FRAMEWORK



IEC 63452 maps and adapts IEC 62443 series standards requirements to the railway application domain and operational environment and details how the requirements are applied in that context. It provides guidance on how the security process can be interfaced with the generic reliability, availability, maintainability and safety (RAMS) life cycle of the IEC 62278 series standards.

ANNEH H provides the description of the railway cybersecurity competence profiles needed to perform Cybersecurity related activities during Railway Application life cycle. The cybersecurity competence profile for railways cybersecurity domain described in this annex have been adapted and tailored from the ECSF.



IEC 63452 DRAFT

ROLE PROFILES & DELIVERABLES



IEC 63452 CD Profile Title	Profile Deliverable	IEC 63452 CD Profile Title	Profile Deliverable
Railway Project Cybersecurity Manager	<ul style="list-style-type: none"> Project Cybersecurity Management Plan Project Cybersecurity Risk Assessment Project Cybersecurity Risk Remediation Action Plan Cybersecurity risk management outcomes and communications with stakeholders Vulnerability Management Plan Project Cybersecurity Case 	Railway Cybersecurity Penetration Tester	<ul style="list-style-type: none"> Threats and Vulnerability Assessment Results Report Penetration Testing Report
Railway Cybersecurity Architect	Cybersecurity Requirements Specification (CRS)	Railway Cybersecurity Assessor	<ul style="list-style-type: none"> Cybersecurity Assessment Plan Cybersecurity Assessment Report
Railway Cybersecurity Risk Analyst	<ul style="list-style-type: none"> Cyber Risk identification and Analysis Cyber Threat risk mitigation Report Cybersecurity acceptance reports 	Railway Cybersecurity Incident Responder	<ul style="list-style-type: none"> Incident Response Plan Cyber Incident Report Lessons & Learnt from Incident response
Railway Cybersecurity Implementer	<ul style="list-style-type: none"> Cybersecurity Solutions Cybersecurity design and service specifications Cybersecurity operation and maintenance manuals Cybersecurity test specifications on design and implementation level 	Railway Cybersecurity Administrator	<ul style="list-style-type: none"> Cybersecurity configuration / administration plan Cybersecurity inventory management plan Cybersecurity configuration sheet Cybersecurity account setting sheet Cybersecurity configuration / administration test report Cybersecurity inventory list Evidence of SecRAC application for Cybersecurity Case

(IEC 63452 DRAFT, ANNEH H)



DEEP DIVE ON EASA STUDY ON APPLICATION OF THE ECSF IN AVIATION

Aviation, like other transport and industrial sectors, is characterised by the coexistence of **two primary classes of technologies** within organisations:

- Information and Communication Technologies (ICT)
- Operational Technologies (OT)



WHY:

The Regulation 2023/203 (Part-IS) for the management of cybersecurity risks with a potential impact on aviation safety. This Regulation sets out requirements for aviation organisations and relevant competent authorities and allows some roles to be described from a workplace perspective by defining mission, deliverables, and tasks.



DEEP DIVE ON EASA STUDY ON APPLICATION OF THE ECSF IN AVIATION OT VS IT

CONVERGENCE:

The gap between them is gradually closing. **OT systems are becoming more similar to ICT systems** due to technology convergence and the adoption of digitalisation in the aviation sector. This convergence involves the **integration of IT practices and technologies into OT systems** to improve efficiency, enhance data analysis capabilities and enable better decision making.

DIFFERENCES:

Cybersecurity Risk Policy: OT risk assessment involves safety and information security, so additional considerations need for the critical safety aspects associated with physical processes and assets

Availability requirements: OT systems are typically required to operate continuously and be resilient to cyber-attacks

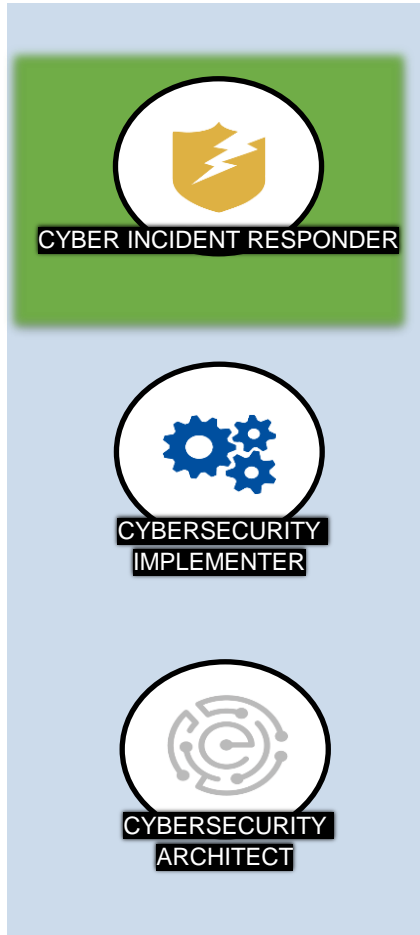
Change Management Process: OT patches sometimes cannot be implemented (in a timely manner)

EASA PROFILES

Profile Title	Deliverable	Part – IS role considerations
Chief Information Security Officer (CISO)	Cybersecurity Strategy / Policy	Responsible Person
Cyber Legal, Policy & Compliance Officer	Compliance Manual / Compliance Report	Compliance Monitoring
Cybersecurity Auditor	Cybersecurity Audit Plan / Report	Auditor within compliance monitoring function
Cybersecurity Risk Manager	Cybersecurity Risk Assessment Report / Remediation Action Plan	One of the “appointed persons”
Cybersecurity Implementer	Cybersecurity Solutions	Not specified, but expected
Cyber Incident Responder	Incident Response Plan / Incident Report	One of the “appointed persons”
Cyber Threat Intelligence Specialist	Cyber Threat Intelligence Manual / Report	Not specified, but expected
Cybersecurity Architect	Cybersecurity Architecture Diagram / Requirements Report	Not specified, but expected
Cybersecurity Educator	Cybersecurity Awareness Program / Training Material	Not specified, but expected
Cybersecurity Researcher	Publication in Cybersecurity	Not foreseen
Digital Forensics Investigator	Digital Forensics Analysis Results / Electronic Evidence	Not specified, but expected
Penetration Tester	Vulnerability Assessment Results Report / Penetration Testing Report	Not specified, may be useful in complex setting

EASA PROFILES

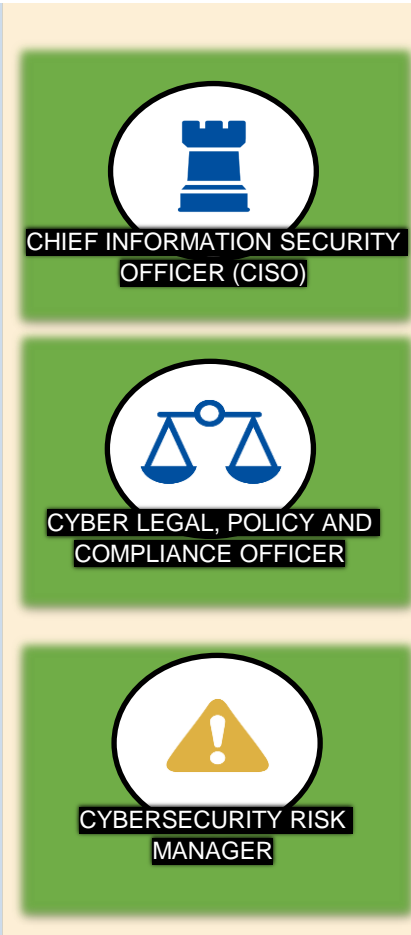
1ST LINE OF DEFENCE



This column contains three roles, each with an icon in a circle above its name. The background is light blue. The roles are: Cyber Incident Responder (shield with lightning bolt), Cybersecurity Implementer (gears), and Cybersecurity Architect (maze).

- CYBER INCIDENT RESPONDER
- CYBERSECURITY IMPLEMENTER
- CYBERSECURITY ARCHITECT

2ND LINE OF DEFENCE



This column contains three roles, each with an icon in a circle above its name. The background is light yellow. The roles are: Chief Information Security Officer (CISO) (castle tower), Cyber Legal, Policy and Compliance Officer (scales), and Cybersecurity Risk Manager (warning triangle).

- CHIEF INFORMATION SECURITY OFFICER (CISO)
- CYBER LEGAL, POLICY AND COMPLIANCE OFFICER
- CYBERSECURITY RISK MANAGER

3RD LINE OF DEFENCE



This column contains one role, Cybersecurity Auditor, with an icon in a circle above its name. The background is light pink.

- CYBERSECURITY AUDITOR

SUPPORTING



This column contains six roles, each with an icon in a circle above its name. The background is light grey. The roles are: Cyber Threat Intelligence Specialist (bug with magnifying glass), Penetration Tester (syringe with binary code), Digital Forensics Investigator (magnifying glass with binary code), Cybersecurity Researcher (flask), and Cybersecurity Educator (graduation cap).

- CYBER THREAT INTELLIGENCE SPECIALIST
- PENETRATION TESTER
- DIGITAL FORENSICS INVESTIGATOR
- CYBERSECURITY RESEARCHER
- CYBERSECURITY EDUCATOR

JOIN ENISA IN THE ECSF JOURNEY CALL UPON STAKEHOLDERS

Foster collaboration with the Ad-Hoc Working Group on ECSF to enhance cybersecurity skills understanding and development across Europe



CONNECT with ENISA to
STRENGTHEN THE ECSF



EUROPEAN
CYBERSECURITY
SKILLS FRAMEWORK



THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Agamemnonos 14, Chalandri 15231,
Attiki, Greece

 • EuSkills@enisa.europa.eu

 • www.enisa.europa.eu

