EUROPEAN UNION AGENCY
FOR CYBERSECURITY

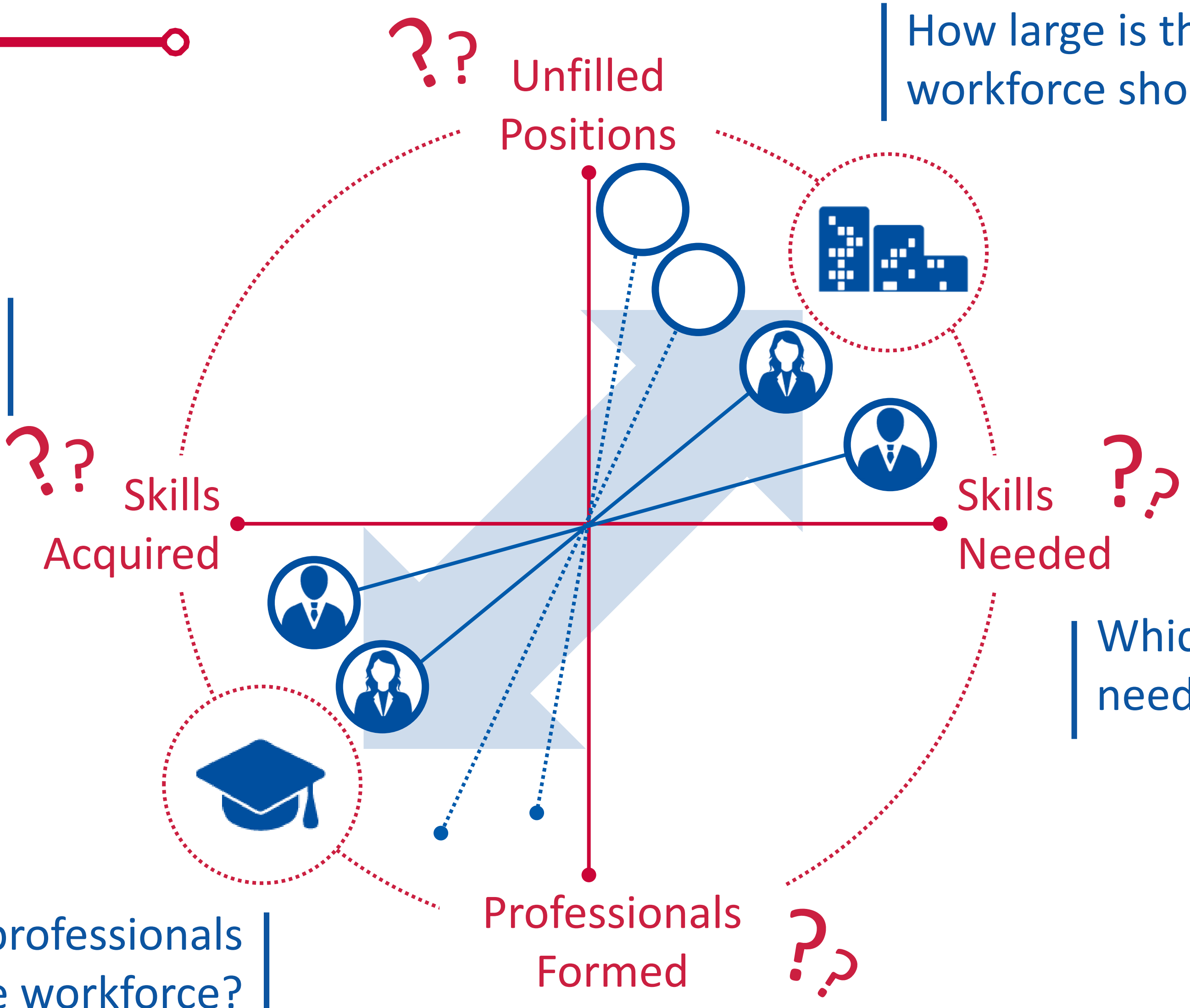
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

Dr. Fabio Di Franco

Cybersecurity skills gap and shortage



How large is the workforce shortage?

Which skills do new professionals need to acquire?

Which skills are needed?

How many professionals join the workforce?

Understanding the cybersecurity skills gaps in the Europe.

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

With this framework we are trying to:

Create a common understanding of the roles, competencies, skills and knowledge

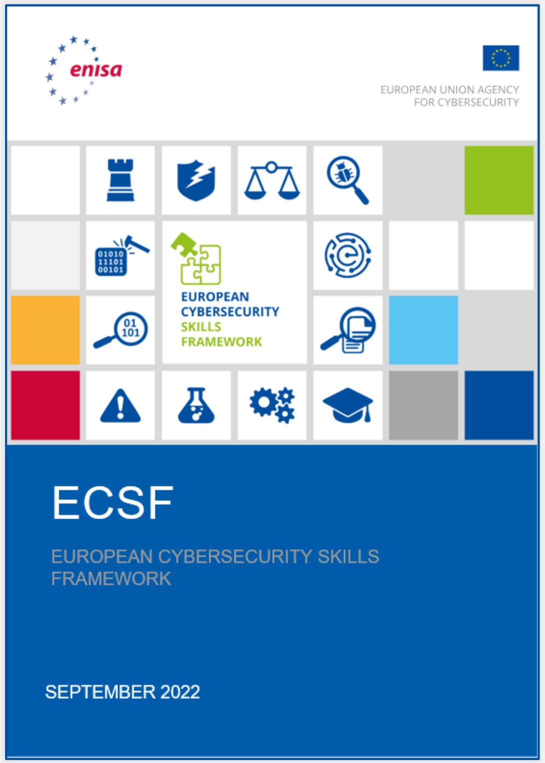
Facilitate cybersecurity skills recognition

Support the design of cybersecurity related training programs

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

The framework consists of 2 documents:



enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

ECSF

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

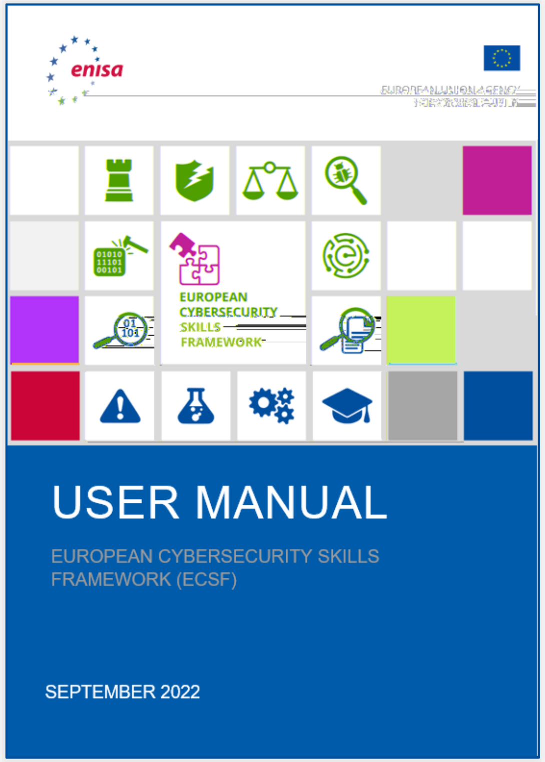
SEPTEMBER 2022

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.



enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

USER MANUAL

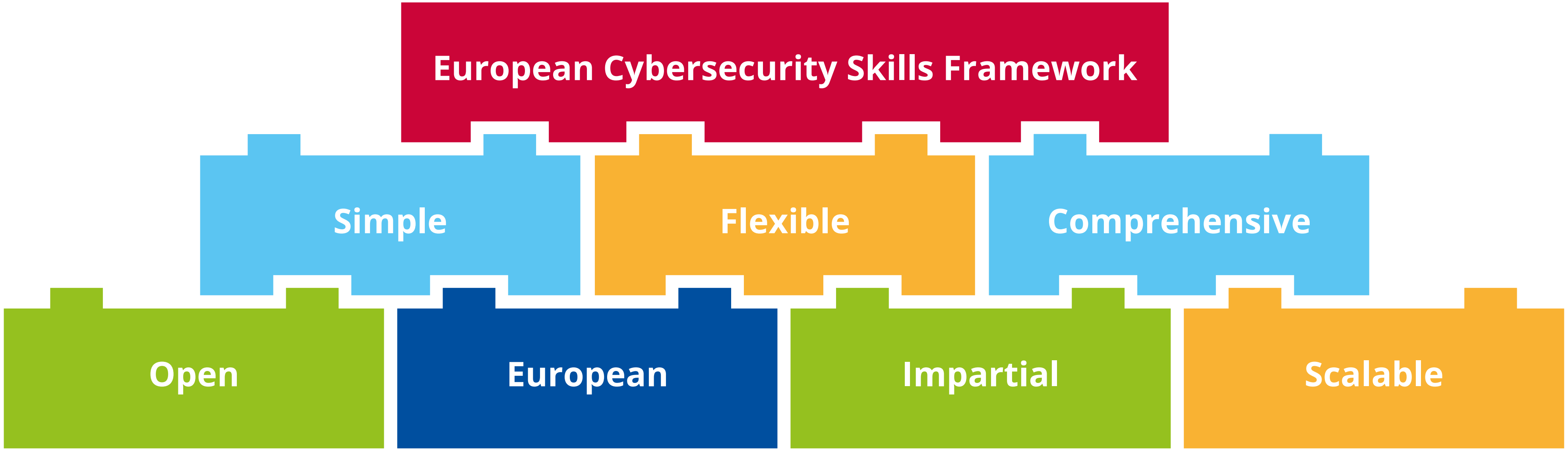
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

SEPTEMBER 2022

https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Principles



With this framework we are trying to:

Create a common understanding of the roles, competencies, skills and knowledge

Facilitate cybersecurity skills recognition

Support the design of cybersecurity related training programs

AD-HOC WORKING GROUP ON THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

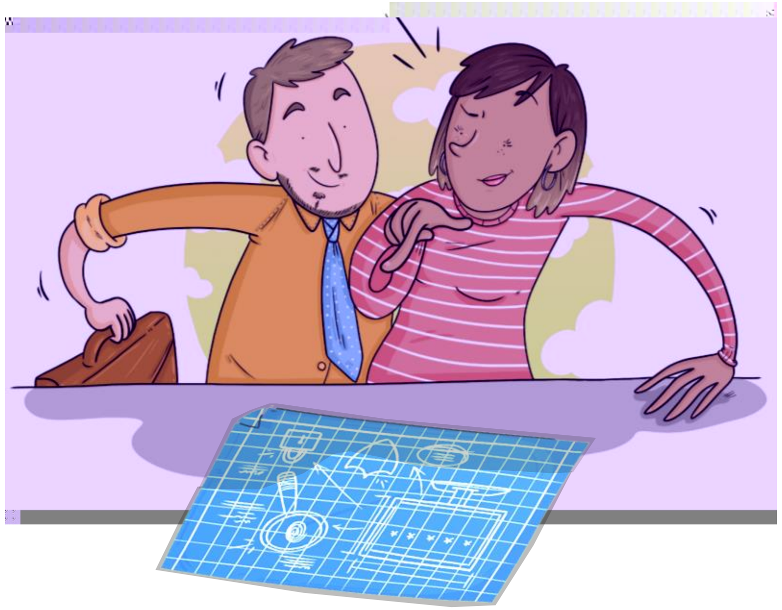
The scope of this ad-hoc working group is to advise and aid ENISA in developing a European Cybersecurity Skills Framework.

17 Experts

13 Countries

Dec 2020 Started

AD-HOC WORKING GROUP MEMBERS & OBSERVERS



Members	Agata BEKIER	Dow
	Vladlena BENSON	Cyber Security Innovation Partnership Aston University
	Jutta BREYER	Breyer publico consulting
	Sara GARCIA	INCIBE - Spanish National Cybersecurity Institute
	Markku KORKIAKOSKI	Netox Ltd
	Csaba KRASZNAY	National University of Public Service
	Haralambos MOURATIDIS	Stockholm University and University of Brighton
	Christina GEORGHIADOU	Eurobank Cyprus
	Erwin ORYE	NATO CCDCOE
	Edmundas PIESARSKAS	L3CE
	Nineta POLEMI	University of Pireaus
	Paresh RATHOD	Laurea University of Applied Sciences Finland
	Antonio SANNINO	Procter & Gamble
	Fred VAN NOORD	Van Noord Consultancy
	Richard WIDH	Ancautus AB
Observers	Nina OLESEN	European Cyber Security Organization (ECSO)
	Jan HAJNY	Sparta - pilot project of the European competence network

12 CYBERSECURITY 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

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

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	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)	
Main task(s)	strategies, policies, aligned with the business strategy to support the organisational objectives val by the senior management of the organisation and ensure their execution System (ISMS) the organisation -related authorities and communities ngs to the senior management incidents

Key skill(s)	s, certifications, standards, methodologies and frameworks -related laws, regulations and legislations champion and lead the execution of a cybersecurity strategy either directly or by leading its outsourcing ance security documents, reports, SLAs and ensure the security objectives -related issues formulate new plans rage people	
Key knowledge	Cybersecurity-related certifications Cybersecurity maturity models Resource management Management practices	
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

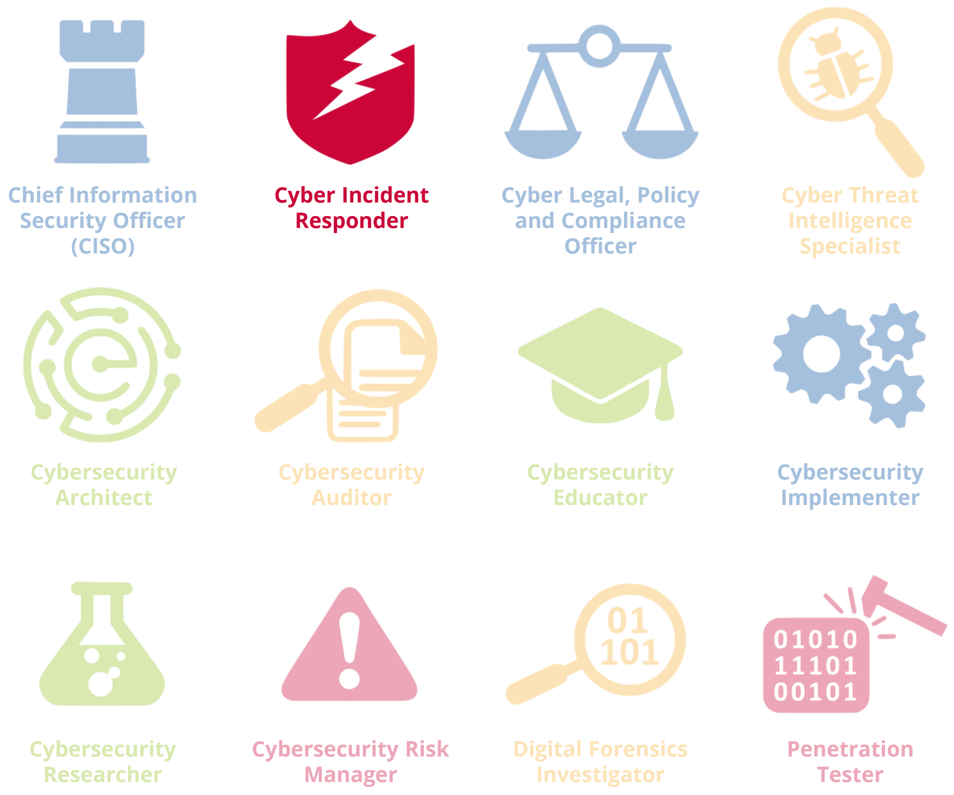
PROFILE OVERVIEW

Cyber Incident Responder

Monitor the organisation’s cybersecurity state, handle incidents during cyber-attacks and assure the continued operations of ICT systems.

Incident Response Plan

Cyber Incident Report



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

PROFILE OVERVIEW

Cyber Legal, Policy and Compliance Officer

Manages compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organisation’s strategy and legal requirements.

Compliance Manual

Compliance Report

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: CYBER LEGAL, POLICY AND COMPLIANCE OFFICER

Profile Title	**Cyber Legal, Policy & Compliance Officer**
Alternative Title(s)	Data Protection Officer (DPO) Privacy Protection Officer Cyber Law Consultant Cyber Legal Advisor Information Governance Officer Data Compliance Officer Cybersecurity Legal Officer IT/ICT Compliance Manager Governance Risk Compliance (GRC) Consultant
Summary statement	Manages compliance with cybersecurity-related standards, legal and regulatory
Mission	Oversees and assures compliance with cybersecurity- and data-related legal, regulatory frameworks and pol governance processes and recommended remediation strategies/solutions to ensure compliance.
Deliverable(s)	Compliance Report
Main task(s)	data protection standards, laws and regulations entify and document compliance gaps upon the privacy policies, procedures owners, holders, controllers, processors, subjects, internal or external partners and entities are informed about their data protection rights, obligations and responsibilities processing to ensure cybersecurity and privacy compliance ties and professional groups and procedures culture of data protection within the organization -party relations

Key skill(s)	requirements Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties rds, frameworks, acknowledged methodologies and tools Explain and communicate data protection and privacy topics to stakeholders and users cybersecurity and data protection strategy and policies	
Key knowledge	s, methodologies and frameworks best practices	
e-Competences (from e-CF)	A.1. Information Systems and Business Strategy Alignment D.1. Information Security Strategy Development E.8. Information Security Management E.9. IS-Governance	Level 4 Level 4 Level 3 Level 4

PROFILE OVERVIEW

Cyber Threat Intelligence Specialist

Collect, process, analyse data and information to produce actionable intelligence reports and disseminate them to target stakeholders.

Cyber Threat Intelligence Manual

Cyber Threat Report

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: CYBER THREAT INTELLIGENCE SPECIALIST

Profile Title	Cyber Threat Intelligence Specialist
Alternative Title(s)	Cyber Intelligence Analyst Cyber Threat Modeller
Summary statement	Collect, process, analyse data and information to produce actionable intelligence reports and disseminate them to target stakeholders.
Mission	Manages cyber threat intelligence life cycle including cyber threat information collection, analysis and production of actionable intelligence and dissemination to security stakeholders and the CTI community, at a tactical, operational and strategic level. Identifies and monitors the Tactics, Techniques and Procedures (TTPs) used non-cyber events can influence cyber-related actions.
Deliverable(s)	
Main task(s)	strategy to Intelligence Requirements intelligence and dissemination to security stakeholders monitor and assess the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors by analysing open-source and proprietary data, information and intelligence n mitigation plans at the tactical, operational and strategic level threats recommendations for Risk Mitigation and cyber threat hunting consequences to non-technical stakeholders

Key skill(s)	borate with other team members and colleagues sources technical analysis and reporting -cyber events with implications on cyber-related activities relevant stakeholders	
Key knowledge	standards, methodologies and frameworks -domain and border-domain knowledge related to cybersecurity persistent cyber threats (APT) -related certifications	
e-Competences (from e-CF)	B.5. Documentation Production D.7. Data Science and Analytics D.10. Information and Knowledge Management E.4. Relationship Management E.8. Information Security Management	Level 3 Level 4 Level 4 Level 3 Level 4

PROFILE OVERVIEW

Cybersecurity Architect

Plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls.

Cybersecurity Architecture Diagram

Cybersecurity Requirements Report

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: CYBERSECURITY ARCHITECT

Profile Title	Cybersecurity Architect
Alternative Title(s)	Cybersecurity Solutions Architect Cybersecurity Designer Data Security Architect
Summary statement	Plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls.
Mission	Designs solutions based on security-by-design and privacy-by-design principles. Creates and continuously improves architectural models and develops appropriate architectural documentation and specifications. Coordinate secure development, integration and maintenance of cybersecurity components in line with standards and other related requirements.
Deliverable(s)	Diagram Report
Main task(s)	rity and privacy requirements -level security architecture design to stakeholders services and products components ensuring the cybersecurity specifications tectures through security reviews and certification merging threats

Key skill(s)	security requirements analysis lyse systems to develop security and privacy requirements and identify effective solutions defaults cybersecurity principles implementers and IT/OT personnel t points of failure across the architecture	
Key knowledge	-related certifications -related requirements analysis Secure development lifecycle -related technologies Cybersecurity risks Cybersecurity trends best practices -Enhancing Technologies (PET) Privacy-by-design standards, methodologies and frameworks	
e-Competences (from e-CF)	A.5. Architecture Design A.6. Application Design B.1. Application Development B.3. Testing B.6. ICT Systems Engineering	Level 5 Level 3 Level 3 Level 3 Level 4

PROFILE OVERVIEW

Cybersecurity Auditor

Perform cybersecurity audits on the organisation's ecosystem. Ensuring compliance with statutory, regulatory, policy information, security requirements, industry standards and best practices.

Cybersecurity Audit Plan

Cybersecurity Audit Report

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: CYBERSECURITY AUDITOR

Profile Title	Cybersecurity Auditor
Alternative Title(s)	Information Security Auditor (IT or Legal Auditor) Governance Risk Compliance (GRC) Auditor Cybersecurity Audit Manager Cybersecurity Procedures and Processes Auditor Information Security Risk and Compliance Auditor Data Protection Assessment Analyst
Summary statement	Ensuring compliance with statutory, regulatory, policy information, security requirements, industry standards and best practices.
Mission	Conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organisation's legal and regulatory frameworks policies. Evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations.
Deliverable(s)	Report
Main task(s)	target environment and manage auditing activities procedures and auditing tests y objectives and requirements based on the risk profile -related applicable laws and regulations -related applicable standards rements and maintenance reports

Key skill(s)	nd deterministic way based on evidence well as technical and organisational controls needs udit with integrity, being impartial and independent	
Key knowledge	best practices ntrols' effectiveness Conformity assessment standards, methodologies and frameworks -related certification -related certifications	
e-Competences (from e-CF)	B.3. Testing B.5. Documentation Production E.3. Risk Management E.6 ICT Quality Management E.8. Information Security Management	Level 4 Level 3 Level 4 Level 4 Level 4

PROFILE OVERVIEW

Cybersecurity Educator

Improves cybersecurity knowledge, skills and competencies of humans.

Cybersecurity Awareness Program

Cybersecurity Training Material

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: CYBERSECURITY EDUCATOR

Profile Title	Cybersecurity Educator
Alternative Title(s)	Cybersecurity Awareness Specialist Cybersecurity Trainer Faculty in Cybersecurity (Professor, Lecturer)
Summary statement	Improves cybersecurity knowledge, skills and competencies of humans.
Mission	Designs, develops and conducts awareness, training and educational programmes in cybersecurity and data protection-related topics. Uses appropriate teaching and training methods, techniques and instruments to communicate and enhance the cybersecurity culture, capabilities, knowledge and skills of human resources. Promotes the importance of cybersecurity and consolidates it into the organisation.
Deliverable(s)	Program Material
Main task(s)	educational material for training and awareness based on content, method, tools, trainees need ction awareness-raising activities, seminars, courses, practical training awareness-raising environments wer continuous enhancement of cybersecurity capacities and capabilities building

Key skill(s)	rsecurity exercises including simulations using cyber range environments -related training resources the awareness, training and education activities	
Key knowledge	-related certifications ity related laws, regulations and legislations	
e-Competences (from e-CF)	D.3. Education and Training Provision D.9. Personnel Development E.8. Information Security Management	Level 3 Level 3 Level 3

PROFILE OVERVIEW

Cybersecurity Implementer

Develop, deploy and operate cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products.

Cybersecurity Solutions

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: CYBERSECURITY IMPLEMENTER

Profile Title	**Cybersecurity Implementer**
Alternative Title(s)	Information Security Implementer Cybersecurity Solutions Expert Cybersecurity Developer Cybersecurity Engineer Development, Security & Operations (DevSecOps) Engineer
Summary statement	Develop, deploy and operate cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products.
Mission	Provides cybersecurity-related technical development, integration, testing, implementation, operation, maintenance, monitoring and support of cybersecurity solutions. Ensures adherence to specifications and conformance requirements, assures sound performance and resolves technical issues required in the -related solutions (systems, assets, software, controls and services), infrastructures and products.
Deliverable(s)	
Main task(s)	-related support to users and customers rsecurity solutions and ensure their sound operation performance of the implemented cybersecurity controls -related actions s technical vulnerabilities

Key skill(s)	security and performance of solutions -related issues	
Key knowledge	programming Operating systems security Computer networks security Offensive and defensive security practices -related technologies	
e-Competences (from e-CF)	A.5. Architecture Design A.6. Application Design B.1. Application Development B.3. Testing B.6. ICT Systems Engineering	Level 3 Level 3 Level 3 Level 3 Level 4

PROFILE OVERVIEW

Cybersecurity Researcher

Research the cybersecurity domain and incorporate results in cybersecurity solutions.

Publication in Cybersecurity

- 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: CYBERSECURITY RESEARCHER

Profile Title	Cybersecurity Researcher
Alternative Title(s)	Cybersecurity Research Engineer Chief Research Officer (CRO) in cybersecurity Senior Research Officer in cybersecurity Research and Development (R&D) Officer in cybersecurity Scientific Staff in cybersecurity Research and Innovation Officer/Expert in cybersecurity Research Fellow in cybersecurity
Summary statement	Research the cybersecurity domain and incorporate results in cybersecurity solutions.
Mission	Conducts fundamental/basic and applied research and facilitates innovation in the cybersecurity domain through cooperation with other stakeholders. Analyses trends and scientific findings in cybersecurity.
Deliverable(s)	
Main task(s)	processes - Manifest and generate research and innovation ideas -of-the-art in cybersecurity-related topics -related solutions prototypes for cybersecurity solutions building and testing a proof of concept to support projects -edge cybersecurity business ideas, services and solutions -related capacity building including awareness, theoretical training, practical training, testing, mentoring, supervising and sharing -sectoral cybersecurity achievements and apply them in a different context or propose innovative approaches and solutions management and budgeting

Key skill(s)	erate new ideas and transfer theory into practice identify effective solutions Monitor new advancements in cybersecurity-related technologies -related issues	
Key knowledge	-related research, development and innovation (RDI) related technologies Multidiscipline aspect of cybersecurity	
e-Competences (from e-CF)	A.7. Technology Trend Monitoring A.9. Innovating D.7. Data Science and Analytics C.4. Problem Management D.10. Information and Knowledge Management	Level 5 Level 5 Level 4 Level 3 Level 3

PROFILE OVERVIEW

Cybersecurity Risk Manager

Manage the organisation's cybersecurity-related risks aligned to the organisation’s strategy. Develop, maintain and communicate the risk management processes and reports.

Cybersecurity Risk Assessment Report

Cybersecurity Risk Remediation Action Plan

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: CYBERSECURITY RISK MANAGER

Profile Title	Cybersecurity Risk Manager
Alternative Title(s)	Information Security Risk Analyst Cybersecurity Risk Assurance Consultant Cybersecurity Risk Assessor Cybersecurity Impact Analyst Cyber Risk Manager
Summary statement	Manage the organisation's cybersecurity- strategy. Develop, maintain and communicate the risk management processes and reports.
Mission	Continuously manages (identifies, analyses, assesses, estimates, mitigates) the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment. Establishes a risk management strategy for the organisation and ensures that risks remain at an acceptable level for the organisation by selecting mitigation actions and controls.
Deliverable(s)	Cybersecurity Risk Remediation Action Plan
Main task(s)	-related threats and vulnerabilities of ICT systems including security controls and risk mitigation and avoidance that best address the port and communicate complete risk management cycle

Key skill(s)	guidelines and ensure compliance with regulations and standards quality and risk management practices - informed decisions to manage and mitigate risks -aware environment nt stakeholders -sharing options	
Key knowledge	es -related certifications -related technologies	
e-Competences (from e-CF)	E.3. Risk Management E.5. Process Improvement E.7. Business Change Management E.9. IS-Governance	Level 4 Level 3 Level 4 Level 4

PROFILE OVERVIEW

Digital Forensics Investigator

Ensure the cybercriminal investigation reveals all digital evidence to prove the malicious activity.

- Digital Forensics Analysis Results
- Electronic Evidence

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: DIGITAL FORENSICS INVESTIGATOR

Profile Title	Digital Forensics Investigator
Alternative Title(s)	Digital Forensics Analyst Cybersecurity & Forensic Specialist Computer Forensics Consultant
Summary statement	Ensure the cybercriminal investigation reveals all digital evidence to prove the malicious activity.
Mission	Connects artefacts to natural persons, captures, recovers, identifies and preserves data, including manifestations, inputs, outputs and processes of digital systems under investigation. Provides analysis, reconstruction and interpretation of the digital evidence based on a qualitative opinion. Presents an unbiased qualitative view without interpreting the resultant findings.
Deliverable(s)	Results Electronic Evidence
Main task(s)	extract, document and analyse digital evidence stakeholders port and present digital forensic analysis findings and results

Key skill(s)	actors t information while preserving its integrity understand way investigation reports	
Key knowledge	Digital forensics recommendations and best practices procedures, standards, methodologies and frameworks Malware analysis tools Cyber threats puter networks security -related certifications	
e-Competences (from e-CF)	A.7. Technology Trend Monitoring B.3. Testing B.5. Documentation Production E.3. Risk Management	Level 3 Level 4 Level 3 Level 3

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

EXAMPLE: PENETRATION TESTER

Profile Title	Penetration Tester
Alternative Title(s)	Pentester Ethical Hacker Vulnerability Analyst Cybersecurity Tester Offensive Cybersecurity Expert Defensive Cybersecurity Expert Red Team Expert Red Teamer
Summary statement	Assess the effectiveness of security controls, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors.
Mission	Plans, designs, implements and executes penetration testing activities and attack scenarios to evaluate the effectiveness of deployed or planned security measures. Identifies vulnerabilities or failures on technical and organisational controls that affect the confidentiality, integrity and availability of ICT products (e.g. systems, hardware, software and services).
Deliverable(s)	Penetration Testing Report
Main task(s)	urity vulnerabilities cybersecurity vulnerabilities ues programs

Key skill(s)	-related issues ate, present and report to relevant stakeholders	
Key knowledge	s -related certifications	
e-Competences (from e-CF)	B.2. Component Integration B.3. Testing B.4. Solution Deployment B.5. Documentation Production E.3. Risk Management	Level 4 Level 4 Level 2 Level 3 Level 4

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

A common language for all
Benefits to target groups   5 steps guide

Jutta Breyer

A COMMON EUROPEAN CYBERSECURITY PROFESSIONAL LANGUAGE FOR ALL

EMPLOYING
The IT Organisation

CAREER CHOICES
The Individual Professional

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

SKILING
Learning Providers

STRATEGIC EMPOWERING
Policy Makers

COMMUNITY BUILDING
Professional Associations

BENEFITS IN THE ORGANISATION

ECSF is useful to

- develop a cybersecurity strategy, organisation structure and HR planning
- specify jobs, role profiles, recruitment offers and needs and other types of specifications
- identify and assess candidates
- perform cybersecurity roles and skills gap analysis and needs forecast at the individual, team or organisational level
- define development and training plans at the individual, team or organisational level
- use a common and realistic language for cybersecurity tenders

BENEFITS TO LEARNING PROVIDERS

ECSF helps to:

- design learning programmes and curricula, re-design and maintain
- collaborate across institutions and enhance learning programme mobility, e.g. cross-European programmes for everyone
- promote learning offerings and raise awareness
- position learning outcomes in real workplace context
- perform assessment and recognition processes
- provide career orientation to students

AT THE INDIVIDUAL PROFESSIONAL LEVEL

People get guidance to

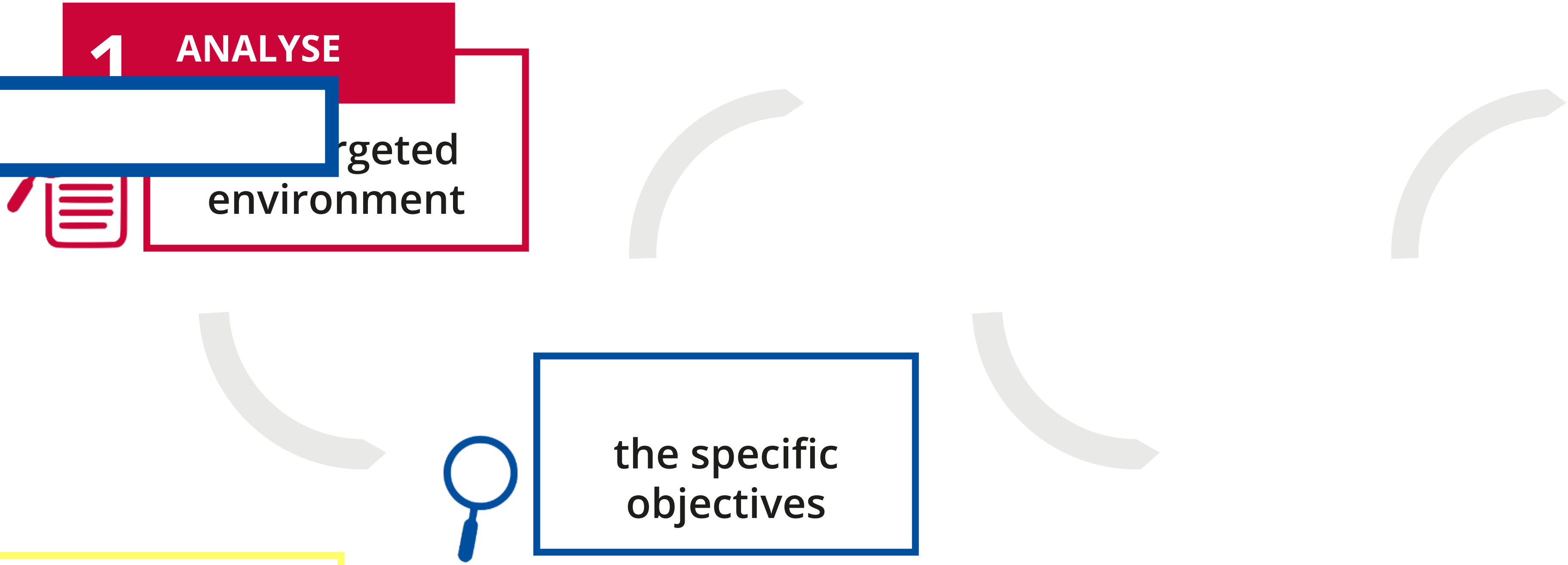
- make professional career choices and position themselves
- support individual life and learning perspective, career paths and professional development needs
- understand Cybersecurity work requirements and expectations in more detail
- identify formal and non-formal learning paths
- get support in skilling from non-technical into technical roles and vice-versa

POLICY MAKERS AND LEGAL STAKEHOLDERS

Get a professional and easy accessible tool to:

- commonly understand the Cybersecurity field
- stimulate priority planning and cybersecurity capacity building
- mapping of multiple cybersecurity initiatives
- support policy initiatives based on data analysis

A BASIC FIVE STEPS GUIDE TO SUCCESSFUL APPLICATION

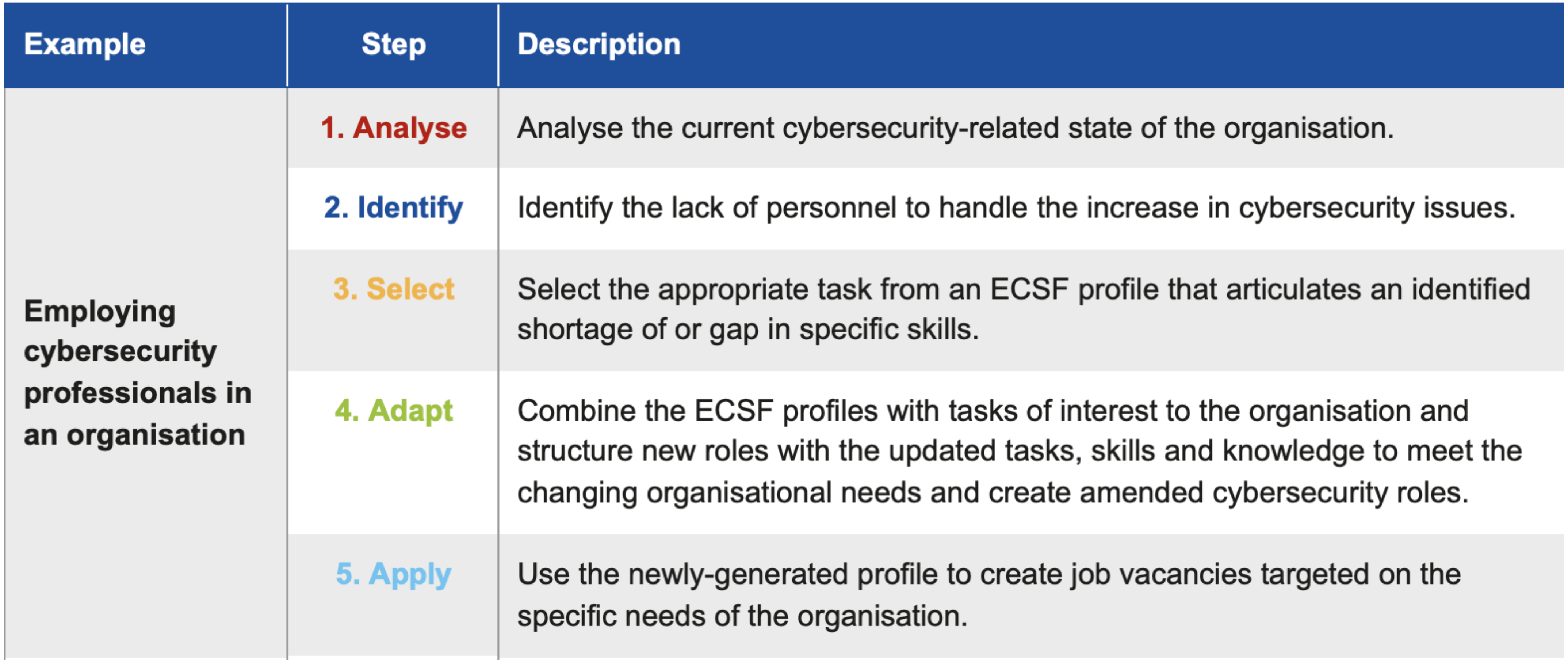


1 ANALYSE

rgeted environment

the specific objectives

ECSF FIVE STEPS GUIDE APPLIED IN THE ORGANISATION

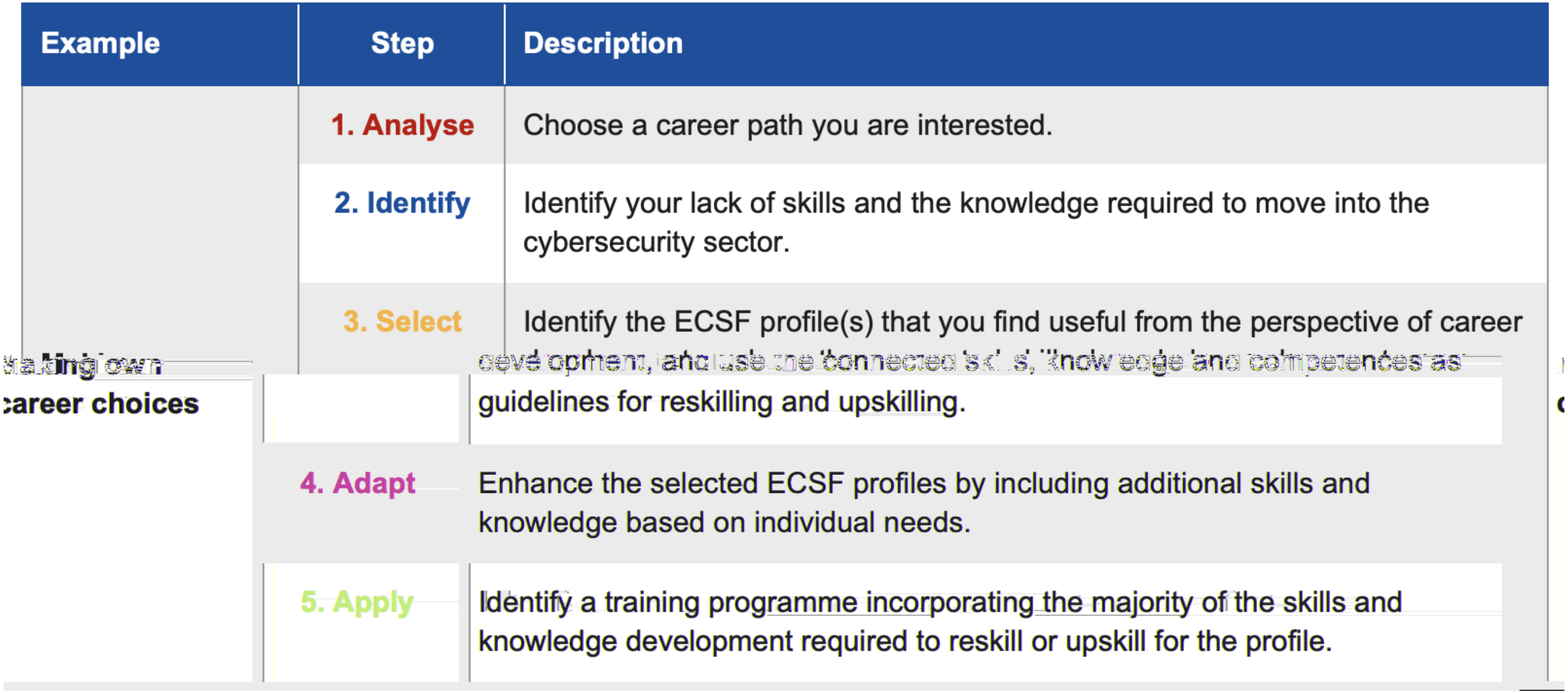


Example	Step	Description
Employing cybersecurity professionals in an organisation	**1. Analyse**	Analyse the current cybersecurity-related state of the organisation.
	2. Identify	Identify the lack of personnel to handle the increase in cybersecurity issues.
	3. Select	Select the appropriate task from 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.

ECSF FIVE STEPS GUIDE APPLIED
IN LEARNING INSTITUTION

Example	Step	Description	
and strategy of the organisation.	Skilling cybersecurity professionals	1. Analyse	Understand the business objectives
ersonnel in cybersecurity related areas.		2. Identify	Identify any lack of expertise and pe
he associated skills and knowledge that		3. Select	Use the ECSF profile(s) to identify t the organisation lacks.
dge from the ECSF to identify the training al to meet the organisation’s needs.		4. Adapt	Analyse selected skills and knowlec needs of a cybersecurity profession
petence of the	5. Apply		Identify training interventions to enhance the com organisation’s workforce.

ECSF FIVE STEPS GUIDE APPLIED
IN THE INDIVIDUAL



Example	Step	Description
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.

A STANDARD REFERENCE FOR EVERYONE

benefit from a common language for everyone and combined action;

accelerate collaboration processes by having a common reference to start from;

a shared reference to gather and present Cybersecurity professional needs related information at all levels, internal and external, at national, European and international levels

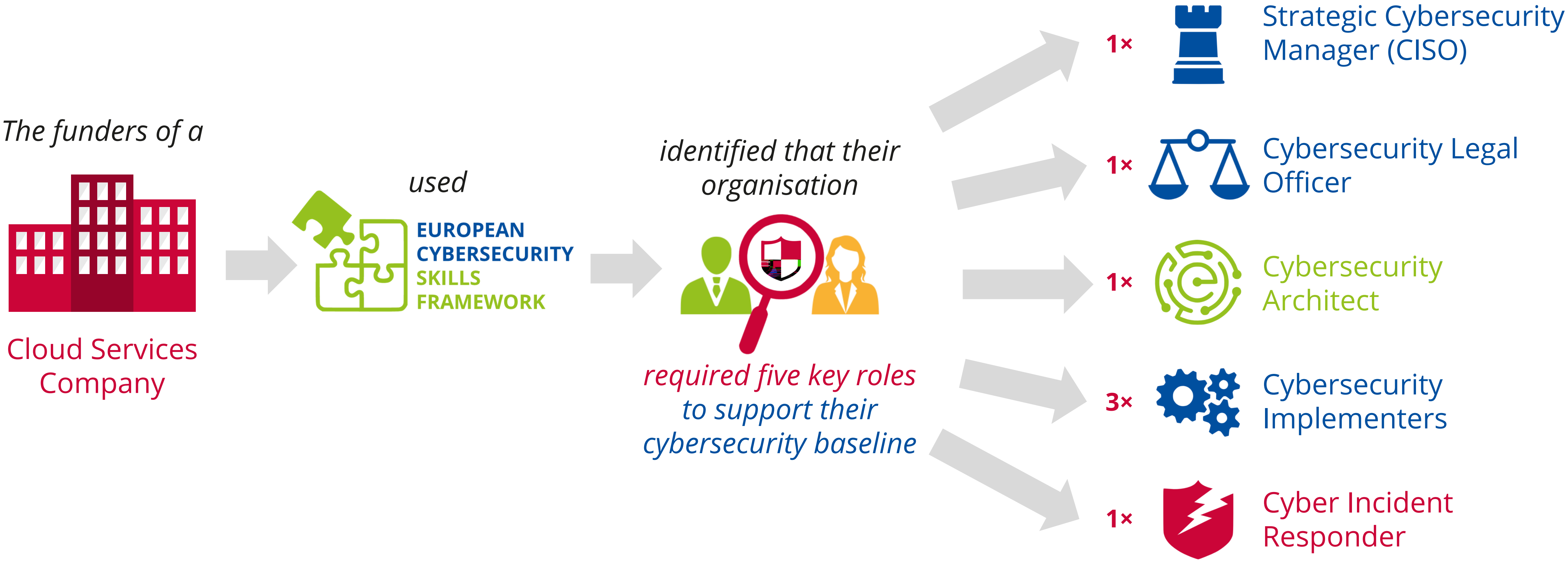
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

Erwin Orye

EXAMPLE I

ENHANCING THE CYBERSECURITY PRACTICES OF A SMALL COMPANY



The funders 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

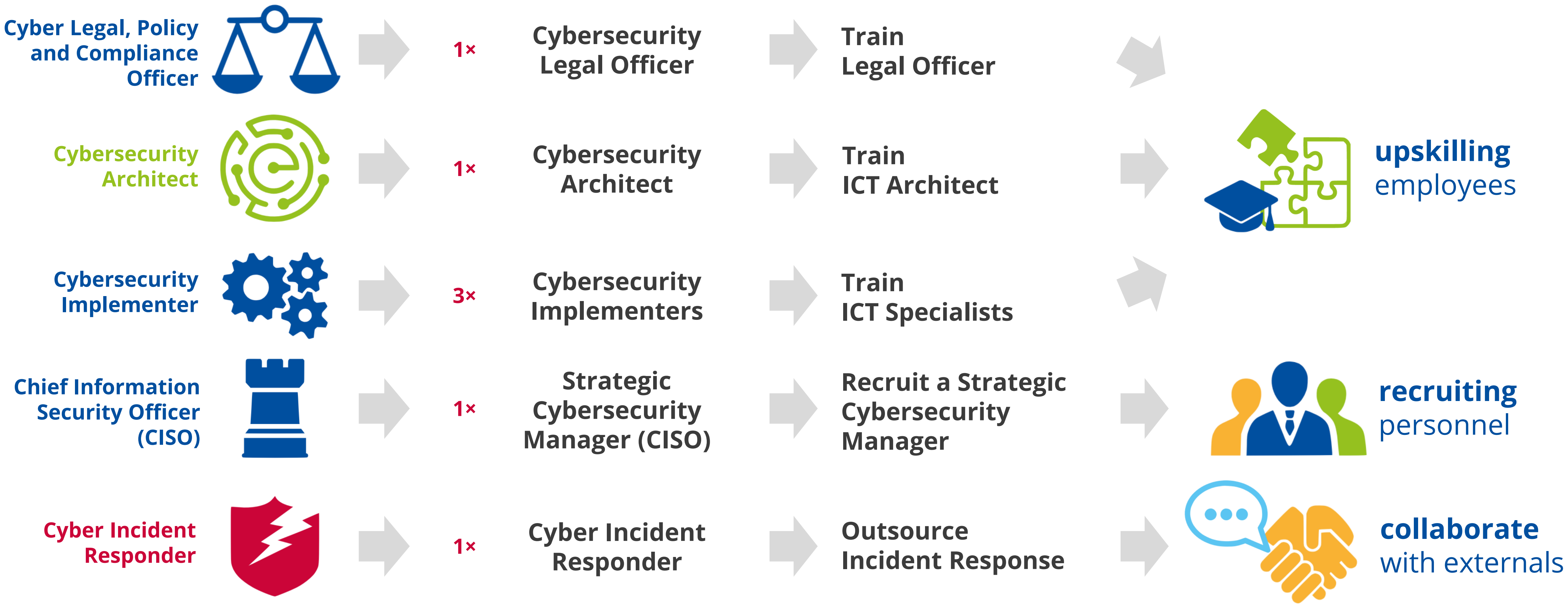
1× Cybersecurity Architect

3× Cybersecurity Implementers

1× Cyber Incident Responder

EXAMPLE I

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	**upskilling** employees
Cybersecurity Implementer	3×	Cybersecurity Implementers	Train ICT Specialists	
Chief Information Security Officer (CISO)	1×	Strategic Cybersecurity Manager (CISO)	Recruit a Strategic Cybersecurity Manager	**recruiting** personnel
Cyber Incident Responder	1×	Cyber Incident Responder	Outsource Incident Response	**collaborate** with externals

EXAMPLE I

ENHANCING THE CYBERSECURITY PRACTICES OF A SMALL COMPANY

cybersecurity **roles** understanding

evaluate **processes** and **structures**

reskilling & **upskilling** employees

cybersecurity **capacity**

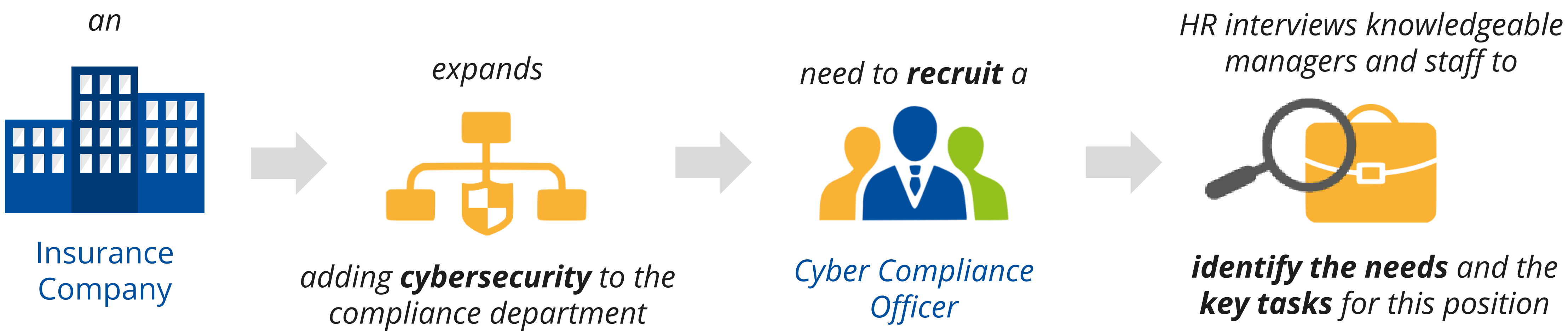
cyber-attacks **resilience**

workforce requirements identification

recruitment supporting

cyber-secure organisation

EXAMPLE II
CRAFTING A JOB DESCRIPTION



an

Insurance Company

expands

*adding **cybersecurity** to the compliance department*

*need to **recruit** a*

Cyber Compliance Officer

HR interviews knowledgeable managers and staff to

***identify the needs** and the **key tasks** for this position*

EXAMPLE II
CRAFTING A JOB DESCRIPTION

Key tasks identified using ECSF for the Cyber Compliance Officer position

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;

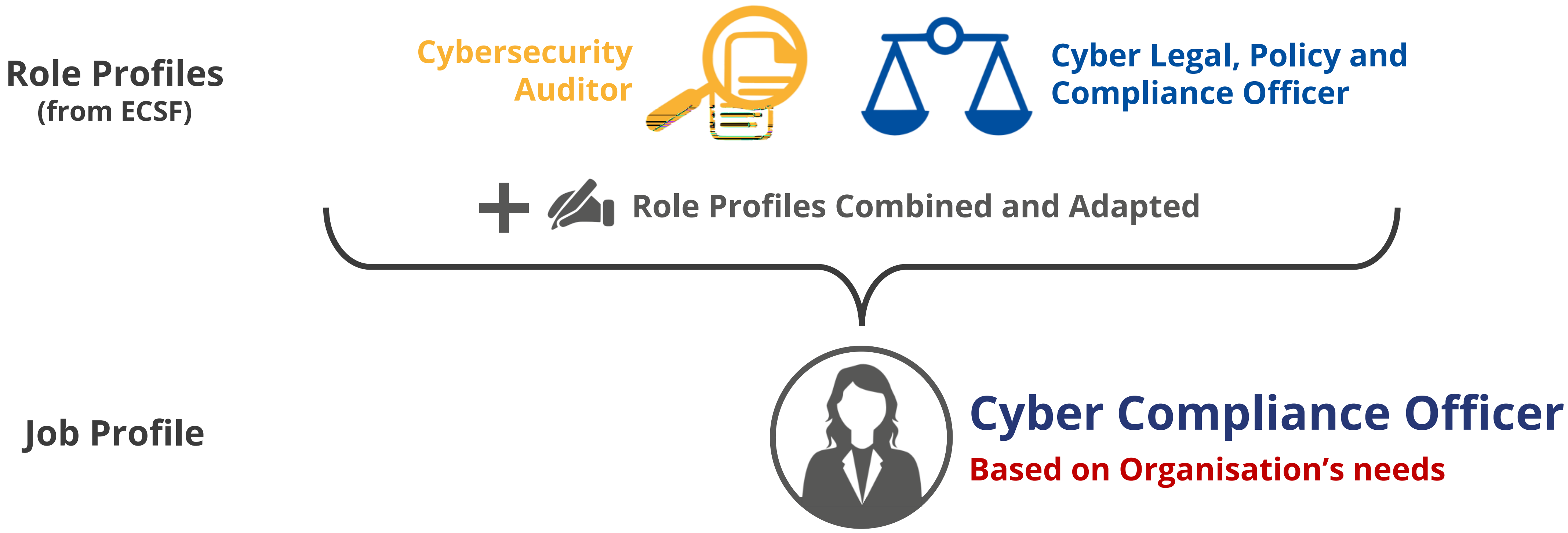
develop an audit plan describing the frameworks, standards, procedures and auditing tests;

execute the audit plan and collect evidence and measurements;

develop and communicate audit results (reporting).

EXAMPLE II
CRAFTING A JOB DESCRIPTION

The HR by analysing different ECSF roles identifies that the key tasks of interest are included the roles of:



Role Profiles
(from ECSF)

Cybersecurity Auditor

Cyber Legal, Policy and Compliance Officer

+ Role Profiles Combined and Adapted

Job Profile

Cyber Compliance Officer

Based on Organisation’s needs

EXAMPLE II

CRAFTING A JOB DESCRIPTION

Cyber Compliance Officer

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

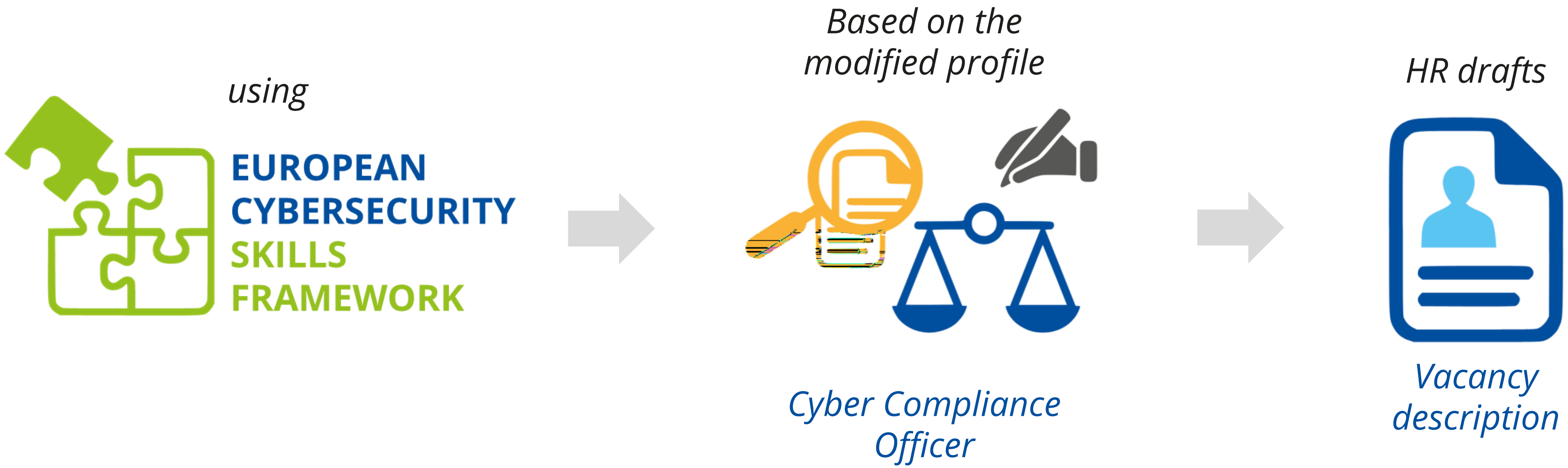
Skills

- understand the implications of modifications of the legal framework to the 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.

EXAMPLE II
CRAFTING A JOB DESCRIPTION



using

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

Based on the modified profile

Cyber Compliance Officer

HR drafts

Vacancy description

EXAMPLE II
CRAFTING A JOB DESCRIPTION

cybersecurity **roles** understanding

workforce requirements identification

role **requirements** identification

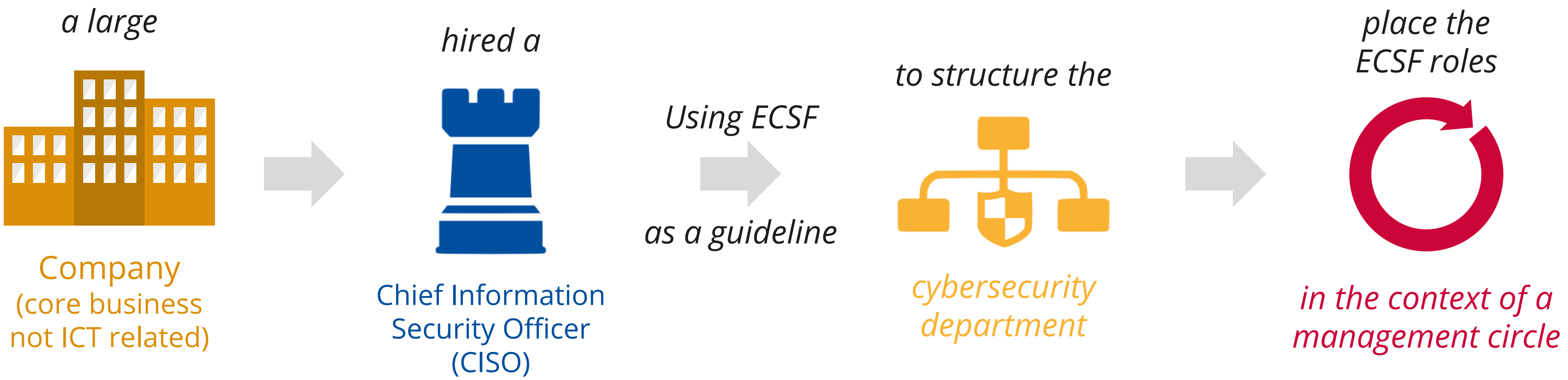
recruitment supporting

custom template building

common language for vacancies

EXAMPLE III

A LARGE CORPORATION WITH ITS MAIN BUSINESS OUTSIDE ICT NEEDS TO SETUP A CYBERSECURITY DEPARTMENT



a large

Company
(core business
not ICT related)

hired a

Chief Information
Security Officer
(CISO)

Using ECSF

as a guideline

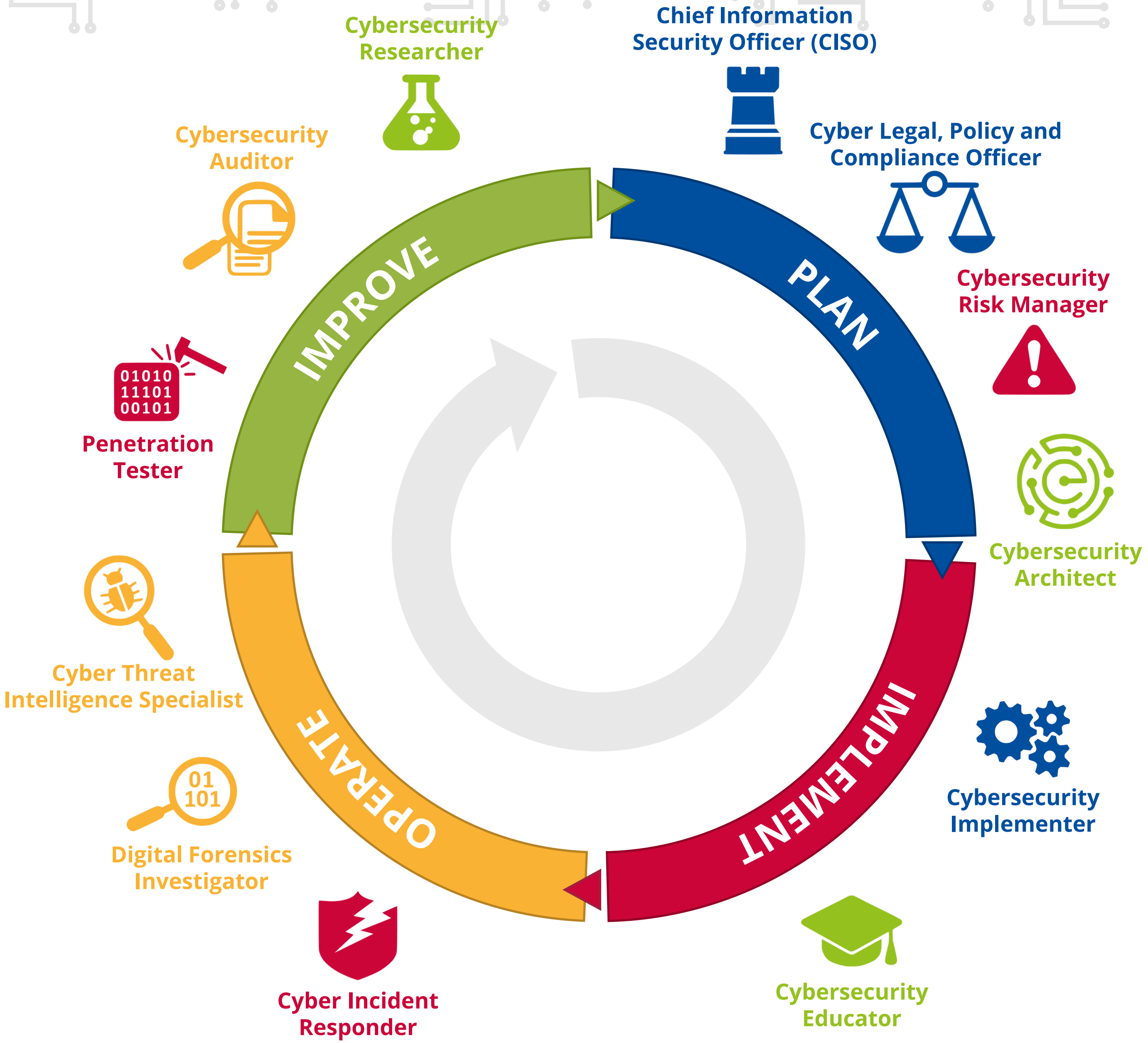
to structure the

cybersecurity department

place the ECSF roles

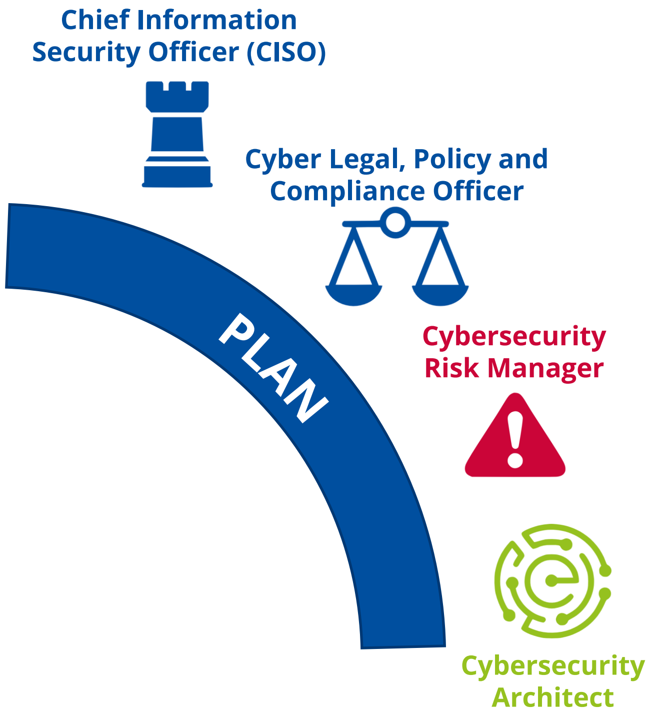
in the context of a management circle

EXAMPLE III


Cybersecurity Researcher
Chief Information Security Officer (CISO)
Cyber Legal, Policy and Compliance Officer
Cybersecurity Auditor
IMPROVE
PLAN
Cybersecurity Risk Manager
01010
11101
00101
Penetration Tester
Cybersecurity Architect
Cyber Threat Intelligence Specialist
OPERATE
IMPLEMENT
Cybersecurity Implementer
01
101
Digital Forensics Investigator
Cyber Incident Responder
Cybersecurity Educator

EXAMPLE III

A LARGE CORPORATION WITH ITS MAIN BUSINESS OUTSIDE ICT NEEDS TO SETUP A CYBERSECURITY DEPARTMENT


Chief Information Security Officer (CISO)
Cyber Legal, Policy and Compliance Officer
PLAN
Cybersecurity Risk Manager
Cybersecurity Architect

In the Plan macro area:

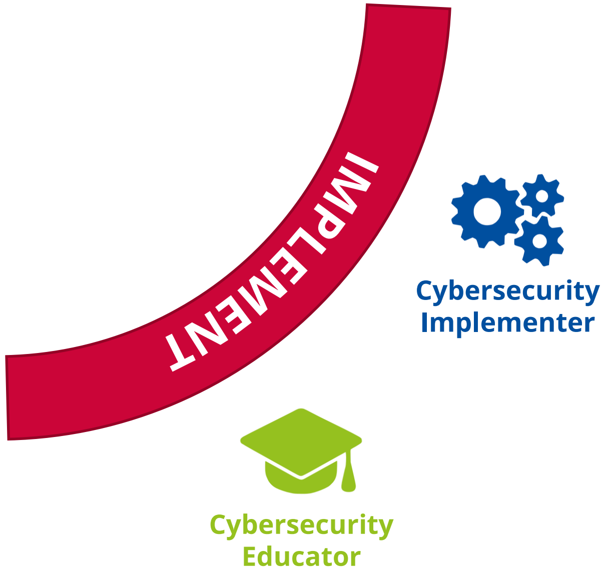
Streamline the organisation structure;

Hire a cybersecurity risk manager to assess the corporate cybersecurity risk posture.

Hire a cybersecurity architect assist defining the overall architecture strategy.

EXAMPLE III

A LARGE CORPORATION WITH ITS MAIN BUSINESS OUTSIDE ICT NEEDS TO SETUP A CYBERSECURITY DEPARTMENT



In the Implementation macro area:

- Upskill or or hire cybersecurity implementors
- Upgrade and train the existing team of instructors towards cybersecurity

EXAMPLE III

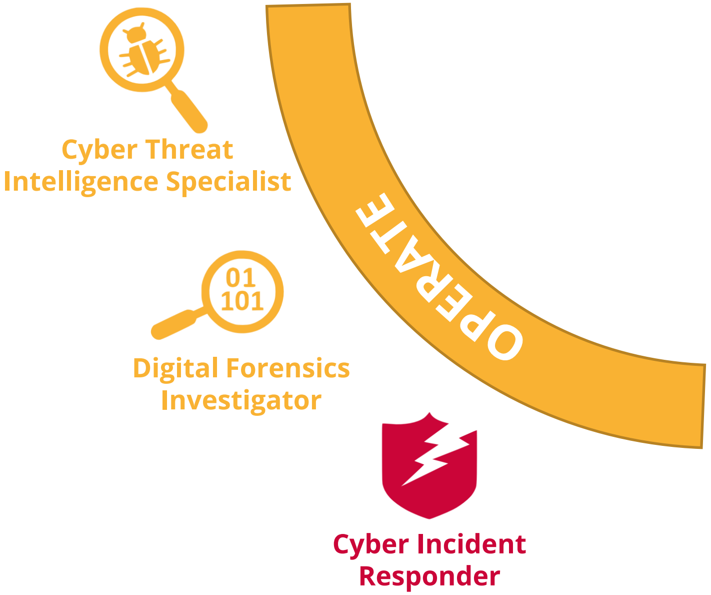
A LARGE CORPORATION WITH ITS MAIN BUSINESS OUTSIDE ICT NEEDS TO SETUP A CYBERSECURITY DEPARTMENT

In the Operate macro area

Set up global security operation centre 24/7.

Engage a specialised consulting company for any forensic needs.

Employ a threat Intelligence specialist to guide hunting for threats and the mitigation of risk.


OPERATE
Cyber Threat Intelligence Specialist
01
101
Digital Forensics Investigator
Cyber Incident Responder

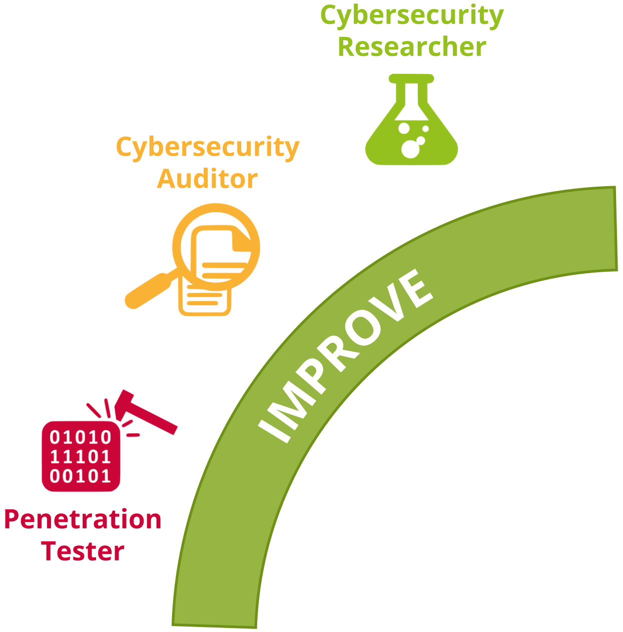
EXAMPLE III
A LARGE CORPORATION WITH ITS MAIN BUSINESS OUTSIDE ICT NEEDS TO SETUP A CYBERSECURITY DEPARTMENT

In the Improve macro area,

Employ an external service provider for penetration testing.

Hire a cybersecurity auditor to audit on security related policies.

No need to hire a cybersecurity researcher.



EXAMPLE III

A LARGE CORPORATION WITH ITS MAIN BUSINESS OUTSIDE ICT NEEDS TO SETUP A CYBERSECURITY DEPARTMENT

cybersecurity **roles** understanding

organisation structure supporting

role **requirements** identification

human resource planning

upskilling employees

assessment of **candidates**

common terminology for collaboration

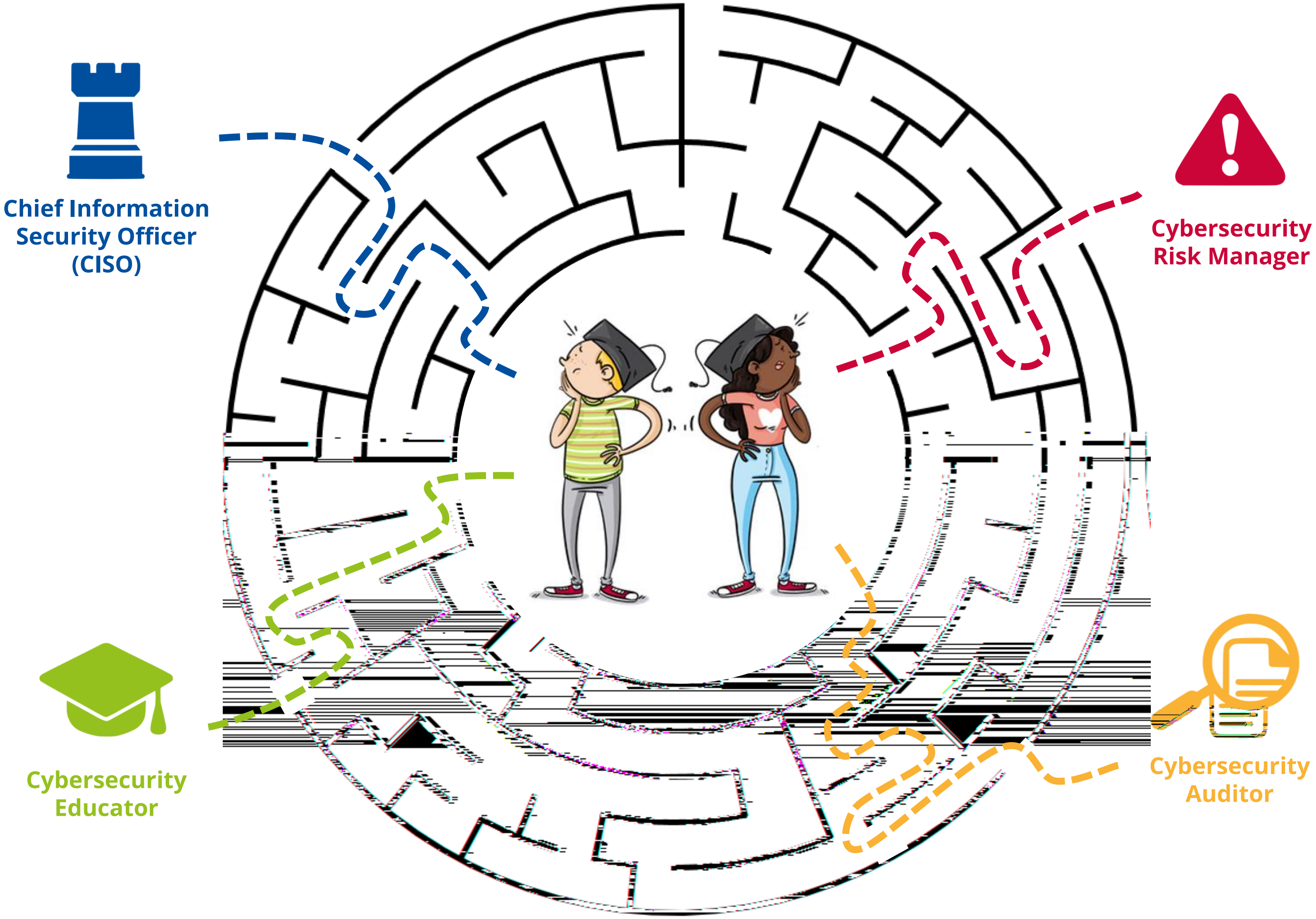
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

Skilling Cybersecurity Professionals
Apply the ECSF as a learning provider

Professor Nineta Polemi

ECSF LINKS EMPLOYMENT WITH EDUCATION



ECSF BEFITS TO LEARNING PROVIDERS

cross institution collaboration

learning programme **mobility**

learning offerings promotion

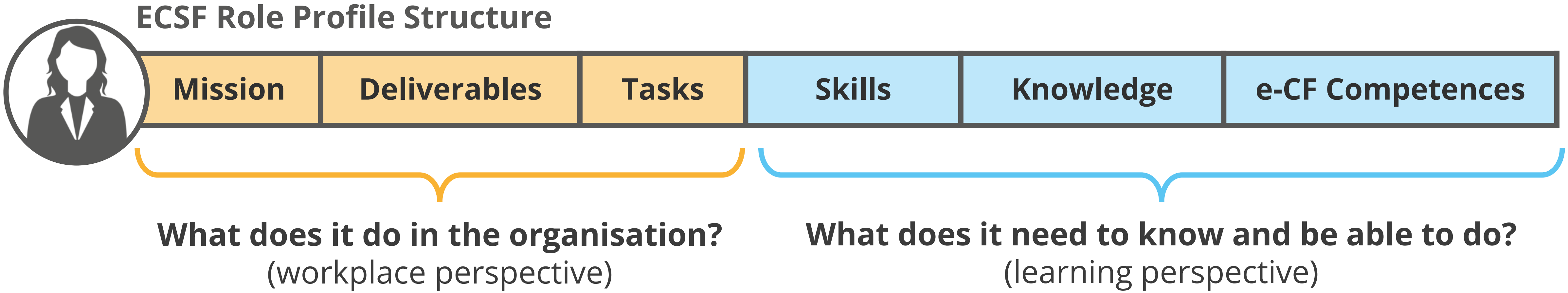
curriculum design supporting

workplace context linking

learning programme assessment

providing **career orientation**

STRUCTURE OF PROFILES LINKS MARKET/EDUCATION REQUIREMENTS



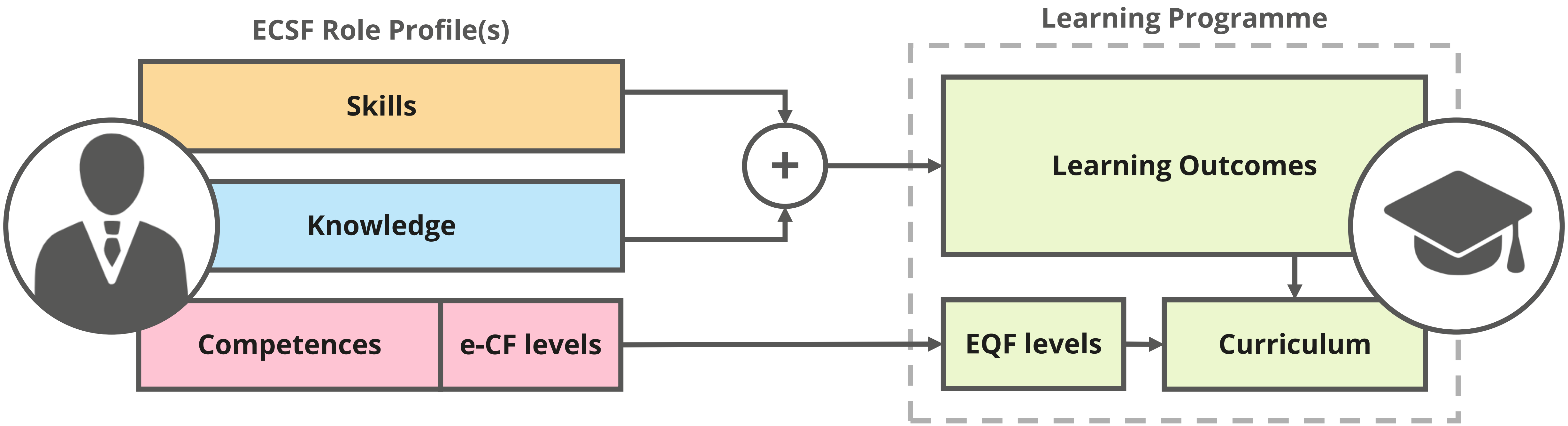
ECSF Role Profile Structure

Mission | Deliverables | Tasks | Skills | Knowledge | e-CF Competences

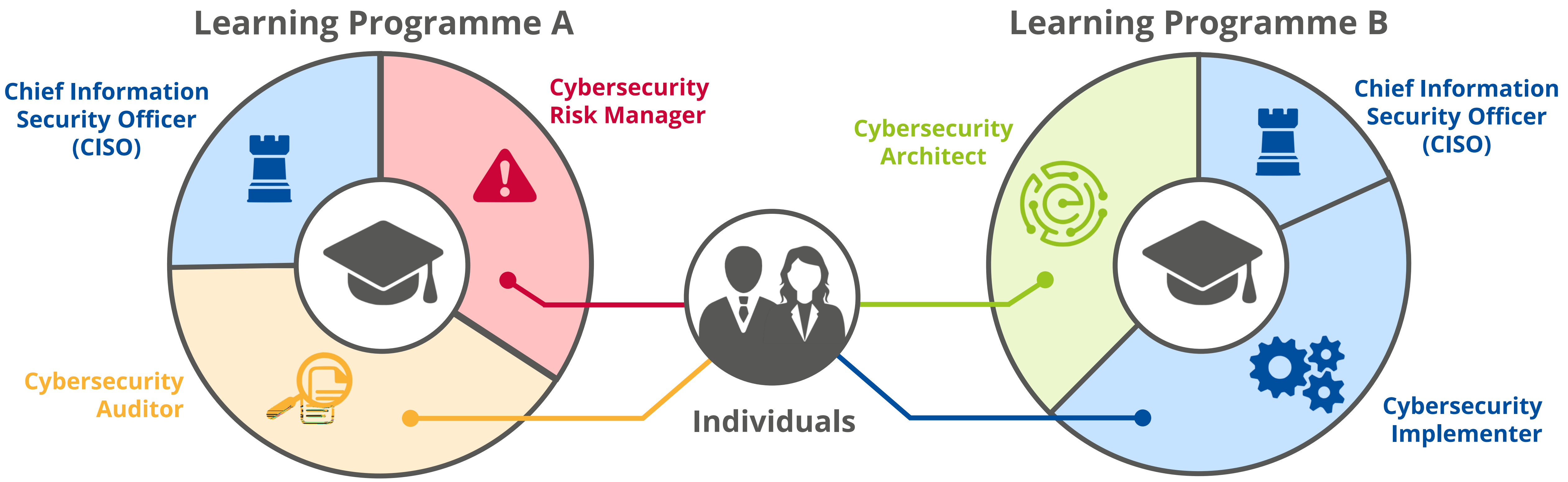
What does it do in the organisation?
(workplace perspective)

What does it need to know and be able to do?
(learning perspective)

ECSF GUIDES LEARNING PROGRAMS



EASILY COMPARE LEARNING PROGRAMS



Learning Programme A

Learning Programme B

Chief Information Security Officer (CISO)

Cybersecurity Risk Manager

Cybersecurity Auditor

Individuals

Cybersecurity Architect

Chief Information Security Officer (CISO)

Cybersecurity Implementer

ECSF EDUCATIONAL BENEFITS SUMMARY

education better serves the market needs

develop targeted curricula

develop joint academic cybersecurity programmes

allow the mobility of trainees and cybersecurity trainers

supports a cross domain and cross industry terminology and view

closes the skills gaps

better prepares trainees for the market

allows people to make better choices

links education outcomes of learning providers
(e.g. HEI, professional bodies, academies, training centres)

THANK YOU FOR YOUR ATTENTION

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

✉ EuSkills@enisa.europa.eu

🌐 www.enisa.europa.eu