enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

European
Cybersecurity
Skills
Framework

ECSF

European Cybersecurity Skills Framework

Draft v0.5
Work In Progress

APRIL 2022

TABLE OF CONTENTS

1. OVERVIEW

Chief Information Security Officer (CISO)

Cyber Incident Responder

Cyber Legal, Policy & Compliance Officer

Cyber Threat Intelligence Specialist

Cybersecurity Architect

Cybersecurity Auditor

Cybersecurity Educator

Cybersecurity Implementer

Cybersecurity Researcher

Cybersecurity Risk Manager

Digital Forensics Investigator

Penetration Tester

2. PROFILES

2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)

Profile Title	**Chief Information Security Officer (CISO)**
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Programme Director Information Security Officer (ISO) Head of Information Security IT Security Officer
Summary statement *Indicates the main purpose of the profile.*	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.
Mission *Describes the rationale of the profile.*	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) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Strategy • Cybersecurity Policy
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• 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) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Understand core organisational business processes • Assess and enhance an organisation's cybersecurity posture • Analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications 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 • Practice ethical cybersecurity organisation requirements

	• Provide practical solutions to cybersecurity issues • Establish a cybersecurity plan • Communicate, coordinate and cooperate with internal and external stakeholders • Apply relevant standards, best practices and legal requirements for information security • Anticipate required changes to the organisation’s information security strategy and formulate new plans • Define and apply maturity models for cybersecurity management • Anticipate future cybersecurity threats, trends, needs and challenges in the organisation • Ability to lead multidisciplinary cybersecurity teams	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of cybersecurity and privacy standards, frameworks, policies, regulations, legislations, certifications and best practices • Understanding of ethical cybersecurity organisation 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	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	D.1. Information Security Strategy Development E.3. Risk Management E.4. Relationship Management E.8. Information Security Management E.9. IS-Governance	Level 5 Level 4 Level 3 Level 4 Level 4

2.2 CYBER INCIDENT RESPONDER

Profile Title	**Cyber Incident Responder**	
Alternative Title(s) *Lists titles under the same profile*	Cyber Incident Handler Security Operations Center (SOC) Analyst Cyber Fighter /Defender Log Files Analyst Security Operation Analyst (SOC Analyst) Cybersecurity SIEM Manager	
Summary statement *Indicates the main purpose of the profile.*	Monitor the organisation's cybersecurity state, manage incidents during cyber-attacks and assure the continued operations of ICT systems.	
Mission *Describes the rationale of the profile.*	Analyses, evaluates and mitigates the impact of cybersecurity incidents. Monitors and assesses systems' cybersecurity state. According to the organisation's Incident Response Plan, restores systems' and processes' functionalities to an operational state.	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cyber Incident Management • Incident Response Plan • Recovery Process • Cyber Incident Report • Vulnerability Management	
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Contribute to the development, maintenance and assessment of the Incident Response Plan • Develop, implement and assess procedures related to incident handling • Identify, analyse, mitigate and communicate cybersecurity incidents • Assess and manage technical vulnerabilities • Measure cybersecurity incidents detection and response effectiveness • Evaluate the resilience of the cybersecurity controls and mitigation actions taken after a cybersecurity or data breach incident • Adopt and develop incident handling testing techniques • Establish procedures for incident results analysis and incident handling reporting • Document incident results analysis and incident handling actions • Cooperate with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) • Cooperate with key personnel for reporting of security incidents according to applicable legal framework	
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Practice all technical, functional and operational aspects of cybersecurity incident handling and response • Work on operating systems, servers, clouds and relevant infrastructures • Work under pressure • Command, communicate and report • Manage and analyse log files	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of cybersecurity incident handling methodologies • Knowledge of cybersecurity incident handling practices and tools • Knowledge of incident handling communication cycle • Knowledge of operating systems internals, networking protocols and services • Knowledge of cybersecurity attacks tactics and techniques • Knowledge of cyber threats and vulnerabilities • Knowledge of legal framework related to cybersecurity and data protection • Knowledge of the operation of Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs)	
e-Competences (from e-CF)	A.7. Technology Trend Monitoring B.2. Component Integration	Level 3 Level 2

For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer	B.3. Testing B.5. Documentation Production C.4. Problem Management	Level 3 Level 3 Level 4

2.3 CYBER LEGAL, POLICY & COMPLIANCE OFFICER

Profile Title	**Cyber Legal, Policy & Compliance Officer**
Alternative Title(s) *Lists titles under the same profile*	Data Protection Officer (DPO) Privacy Protection Officer Cyber Law Consultant Information Governance Officer Data Compliance Officer Cybersecurity Lawyer IT Compliance Manager
Summary statement *Indicates the main purpose of the profile.*	Manages compliance with cybersecurity-related standards, legal and regulatory frameworks based on the organisation's strategy and legal requirements.
Mission *Describes the rationale of the profile.*	Oversees and assures compliance with cybersecurity- and data-related legal, regulatory frameworks and policies in line with the organisation's strategy and legal requirements. Contributes to the organisation's data protection related actions. Provides legal advice in the development of the organisation's cybersecurity governance processes.
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Data Protection Policy
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations • Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures • Enforce and advocate organisation's data privacy and protection program • Ensure that data owners, holders, controllers, processors, subjects, internal or external partners and entities are informed about their data protection rights, obligations and responsibilities • Act as a key contact point to handle queries and complaints regarding data processing • Assist in designing, implementing, auditing and compliance testing activities in order to ensure cybersecurity and privacy compliance • Monitor audits and data protection related training activities • Cooperate and share information with authorities and professional groups • Contribute to the development of the organisation's cybersecurity strategy, policy and procedures • Manage legal aspects of information security responsibilities and third-party relations
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements • Abilities to carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy • Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties • Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools • Ability to explain and communicate data protection and privacy topics to stakeholders and users • Understand, practice and adhere to ethical requirements and standards • Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies • Work as part of a team and collaborate with colleagues

Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of information security • Advanced knowledge of data privacy and protection laws and regulations • Advanced knowledge of National, EU and international cybersecurity and related privacy standards, legislation, policies and regulations • Knowledge of legal compliance requirements and practices • Knowledge of privacy impact assessment methodologies • Basic understanding of data storage, processing and protections within systems, services and infrastructures	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	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

2.4 CYBER THREAT INTELLIGENCE SPECIALIST

Profile Title	**Cyber Threat Intelligence Specialist**
Alternative Title(s) *Lists titles under the same profile*	Cyber Intelligence Analyst Cyber Threat Modeller
Summary statement *Indicates the main purpose of the profile.*	Collect, process, analyse data and information to produce actionable intelligence reports and disseminate them to target stakeholders.
Mission *Describes the rationale of the profile.*	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 by cyber threat actors and their trends, track threat actors' activities and observe how non-cyber events can influence cyber-related actions.
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cyber Intelligence Analysis • Cyber Threat Intelligence Management • Cyber Threat Report
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Develop, implement and manage the organisation's cyber threat intelligence strategy • Develop plans and procedures to manage threat intelligence • Translate business requirements into Intelligence Requirements • Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders • Identify and assess cyber threat actors targeting the organisation • Identify, monitor and assess the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors by analysing open-source and proprietary data, information and intelligence • Produce actionable reports based on threat intelligence data • Elaborate and advise on mitigation plans at the tactical, operational and strategic level • Coordinate with stakeholders to share and consume intelligence on relevant cyber threats • Leverage intelligence data to support and assist with threat modelling, recommendations for Risk Mitigation and cyber threat hunting • Articulate and communicate intelligence openly and publicly at all levels • Convey the proper security severity by explaining the risk exposure and its consequences to non-technical stakeholders
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Work in a team and cooperate with different external Subject Matter Experts whenever needed • Collect, analyse and correlate cyber threat information originating from multiple sources • Identify threat actors TTPs and campaigns • Automate threat intelligence management procedures • Conduct technical analysis and reporting • Identify non-cyber events with implications on cyber-related activities • Model threats, actors and TTPs • Write and communicate intelligence reports to stakeholders • Use and apply CTI platforms and tools
Key knowledge *A list of essential knowledge required to perform work functions and*	• Advanced knowledge of IT/OT, operating systems and computer networks • Advanced knowledge of cybersecurity solutions • Knowledge of TTP frameworks • Knowledge of big data handling and analytics methods

duties by the profile. *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of scripting and programming languages • Advanced knowledge of CTI sharing standards • Knowledge of recent vulnerability disclosures, data breach incidents and geopolitical events impacting cyber risk • Knowledge of advanced and persistent cyber threats and threat actors • Knowledge of statistics and forecasting methodologies	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	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

2.5 CYBERSECURITY ARCHITECT

Profile Title	**Cybersecurity Architect**
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Solutions Architect Cybersecurity Designer Data Security Architect
Summary statement *Indicates the main purpose of the profile.*	Plans and designs security-by-design solutions (infrastructures, systems, assets, software, hardware and services) and cybersecurity controls.
Mission *Describes the rationale of the profile.*	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) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Architecture • Cybersecurity Requirements
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Design and propose a secure architecture to implement the organisation's strategy • Develop organisation's cybersecurity architecture to address security and privacy requirements • Produce architectural documentation and specifications • Present high-level security architecture design to stakeholders • Establish a secure environment during the development lifecycle of systems, services and products • Coordinate the development, integration and maintenance of cybersecurity components ensuring the cybersecurity specifications • Analyse and evaluate the cybersecurity of the organisation's architecture • Assure the security of the solution architectures through security reviews and certification • Collaborate with other teams and colleagues • Evaluate the impact of cybersecurity solutions on the design and performance of the organisation's architecture • Adapt the organisation's architecture to emerging threats • Assess the implemented architecture to maintain an appropriate level of security
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Conduct user and business requirements analysis • Draw architectural and functional specifications • Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles • Guide and communicate with implementers and IT/OT personnel • Report, communicate and present to stakeholders • Propose cybersecurity architectures based on stakeholder's needs and budget • Select appropriate specifications, procedures and controls • Build resilience against points of failure across the architecture • Provide technological design leadership • Coordinate the integration of security solutions
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level) Basic Understanding of: Understanding of:*	• Understanding of organisation's mission and business objectives risks • Understanding of security-related standards and requirements • Knowledge of secure development lifecycle • Knowledge of security architecture reference models and security solutions • Knowledge of security technologies and solutions • Knowledge of cybersecurity risks and threats • Knowledge of the latest cybersecurity trends • Understanding of cybersecurity-related standards and compliance requirements • Knowledge of legacy security techniques

Knowledge of: *Advanced knowledge of:*	• Knowledge of Privacy-Enhancing Technologies (PET) • Knowledge of privacy-by-design methodologies	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	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

2.6 CYBERSECURITY AUDITOR

Profile Title	**Cybersecurity Auditor**
Alternative Title(s) *Lists titles under the same profile*	Information Security Auditor Cybersecurity Audit Manager Cybersecurity Procedures and Processes Auditor Source Code Review Auditor Information Security Risk and Compliance Auditor Data Protection Assessment Analyst
Summary statement *Indicates the main purpose of the profile.*	Perform cybersecurity audits on the organisation’s ecosystem.
Mission *Describes the rationale of the profile.*	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) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Audit Plan • Cybersecurity Audit
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Develop the organisation's auditing policy, procedures, standards and guidelines • Establish the methodologies and practices used for systems auditing • Establish the target environment and manage auditing activities • Define audit scope, objectives and criteria to audit against • Develop an audit plan describing the frameworks, standards, methodology, procedures and auditing tests • Review target of evaluation, security objectives and requirements based on the risk profile • Audit compliance with cybersecurity-related applicable laws and regulations • Audit conformity with cybersecurity-related applicable standards • Execute the audit plan and collect evidence and measurements • Maintain and protect the integrity of audit records • Develop and communicate conformity assessment, assurance, audit, certification and maintenance reports
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Organise and work in a systematic and deterministic way based on evidence • Follow and practice auditing frameworks, standards and methodologies • Apply auditing tools and techniques • Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls • Communicate, explain and adapt legal and regulatory requirements and business needs • Plan and conduct interviews in a systematic and deterministic manner • Collect, evaluate, maintain and protect auditing information • Audit with integrity, being impartial and independent
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:*	• Knowledge of cybersecurity solutions, technical and organisational controls • Knowledge of security controls frameworks, standards • Knowledge of conformity assessment methodologies • Advanced knowledge of auditing frameworks, standards, methodologies and certifications • Knowledge of interviewing techniques

Advanced knowledge of:		
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	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

2.7 CYBERSECURITY EDUCATOR

Profile Title	Cybersecurity Educator
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Awareness Specialist Cybersecurity Trainer Professor of Cybersecurity Lecturer in Cybersecurity
Summary statement *Indicates the main purpose of the profile.*	Improves cybersecurity knowledge, skills and competencies of humans.
Mission *Describes the rationale of the profile.*	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) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Awareness • Cybersecurity Trainings • Cybersecurity Education
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need • Organise, design and deliver cybersecurity and data protection awareness-raising activities, seminars, courses, practical training • Monitor, evaluate and report training effectiveness • Evaluate and report trainee's performance • Finding new approaches for education, training and awareness-raising • Design, develop and deliver cybersecurity simulations, virtual labs or cyber range environments • Provide guidance on cybersecurity certification programs for individuals • Continuously maintain and enhance expertise; encourage and empower continuous enhancement of cybersecurity capacities and capabilities building
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Identify needs in cybersecurity awareness, training and education • Analyse and deliver cybersecurity education and training • Design, develop and deliver cybersecurity curricula and programmes to meet the organisation and individuals' needs • Develop advanced cybersecurity exercises and scenarios for simulations, virtual or cyber range environments • Provide training towards cybersecurity and data protection professional certifications • Deliver training utilising various training resources • Develop evaluation programs for the awareness, training and education activities • Communicate or author publications, reports, training material • Identify and select appropriate pedagogical approaches for the intended audience • Motivate and incentivise learners
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of pedagogical methods • Advanced knowledge of cybersecurity awareness, education and training programme development • Knowledge of cybersecurity-related professional certifications • Knowledge of cutting-edge methods, tools and techniques on hands-on cybersecurity education and training • Knowledge of cybersecurity-related legal framework, regulations, standards • Knowledge of cybersecurity frameworks, methodologies, controls and best practices

e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	D.3. Education and Training Provision D.9. Personnel Development E.8. Information Security Management	Level 3 Level 3 Level 3

2.8 CYBERSECURITY IMPLEMENTER

Profile Title	Cybersecurity Implementer	
Alternative Title(s) *Lists titles under the same profile*	Information Security Implementer Cybersecurity Solutions Expert Cybersecurity Developer Security Engineer Development, Security & Operations (DevSecOps) Engineer	
Summary statement *Indicates the main purpose of the profile.*	Develop, deploy and operate cybersecurity solutions (systems, assets, software, controls and services) on infrastructures and products.	
Mission *Describes the rationale of the profile.*	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 organisation's cybersecurity-related solutions (systems, assets, software, controls and services), infrastructures and products.	
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Solutions Development • Cybersecurity Solutions Deployment • Cybersecurity Solutions Operation	
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Develop, implement, maintain, upgrade, test cybersecurity products • Provide cybersecurity-related support to users and customers • Integrate cybersecurity solutions and ensure their sound operation • Securely configure systems, services and products • Maintain and upgrade the security of systems, services and products • Implement cybersecurity procedures and controls • Monitor and assure the performance of the implemented cybersecurity controls • Document and report on the security of systems, services and products • Work close with the IT/OT personnel on cybersecurity-related actions • Implement, apply and manage patches to products to address technical vulnerabilities	
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Document, report present and communicate with various stakeholders • Integrate cybersecurity solutions to the organisation's infrastructure • Configure solutions according to the organisation's security policy • Assess the security and performance of solutions • Develop and test secure code and scripts • Identify and troubleshoot cybersecurity-related issues • Collaborate with other team members and colleagues	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of systems development life cycle • Knowledge of programming languages • Knowledge of operating systems security • Knowledge of computer networks security • Knowledge of security controls • Knowledge of offensive and defensive security practices • Knowledge of secure coding practices • Knowledge of test methodologies and practices	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-*	A.5. Architecture Design A.6. Application Design B.1. Application Development B.3. Testing	Level 3 Level 3 Level 3 Level 3

CF Explorer: https://ecfusertool.itprofessionalism.org/explorer	B.6. ICT Systems Engineering	Level 4

2.9 CYBERSECURITY RESEARCHER

Profile Title	Cybersecurity Researcher
Alternative Title(s) *Lists titles under the same profile*	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 *Indicates the main purpose of the profile.*	Research the cybersecurity domain and incorporate results in cybersecurity solutions.
Mission *Describes the rationale of the profile.*	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) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Research in Cybersecurity
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Analyse and assess cybersecurity technologies, solutions, developments and processes • Conduct research, innovation and development work in cybersecurity-related topics• Manifest and generate research and innovation ideas • Advance the current state-of-the-art in cybersecurity-related topics • Assist in the development of innovative cybersecurity-related solutions • Conduct experiments and develop a proof of concept, pilots and prototypes for cybersecurity solutions • Select and apply frameworks, methods, standards, tools and protocols including a building and testing a proof of concept to support projects • Contributes towards cutting-edge cybersecurity business ideas, services and solutions • Assist in cybersecurity-related capacity building including awareness, theoretical training, practical training, testing, mentoring, supervising and sharing • Identify cross-sectoral cybersecurity achievements and apply them in a different context or propose innovative approaches and solutions • Lead or participate in the innovation processes and projects including project management and budgeting • Publish and present scientific works and research and development results
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Generate new ideas and transfer theory into practice • Decompose, analyse systems, spot weaknesses, develop security and privacy requirements and identify effective or ineffective related solutions • Analyse and solve complex problems and security challenges • Continuously monitor new advancements and cybersecurity innovations • Communicate and disseminate the scientific outcomes • Prove the soundness of the research results • Collaborate with other team members
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level) Basic Understanding of:*	• Knowledge of research, development and innovation (RDI) relevant to cybersecurity subject matters • Knowledge of cybersecurity methods, methodologies, tools and techniques • Knowledge of project management and budgeting • Knowledge of programs and grants • Understanding of copyright and intellectual property rights issues, standards and patent filing • Understanding of the multidiscipline aspect of cybersecurity

Understanding of: *Knowledge of:* *Advanced knowledge of:*	• Understanding of responsible disclosure of cybersecurity-related information • Understanding of espionage and coercion threats and risk in international research	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	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

2.10 CYBERSECURITY RISK MANAGER

Profile Title	**Cybersecurity Risk Manager**
Alternative Title(s) *Lists titles under the same profile*	Information Security Risk Analyst Cybersecurity Risk Assurance Consultant Cybersecurity Risk Assessor Cybersecurity Impact Analyst
Summary statement *Indicates the main purpose of the profile.*	Manage the organisation's cybersecurity-related risks aligned to the organisation's strategy. Develop, maintain and communicate the risk management processes and reports.
Mission *Describes the rationale of the profile.*	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) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Risk Management
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Develop an organisation's cybersecurity risk management strategy • Manage an inventory of organisation's assets • Identify and assess cybersecurity-related threats and vulnerabilities of ICT systems • Identification of threat landscape including attackers' profiles and estimation of attacks' potential • Assess cybersecurity risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy • Monitor effectiveness of cybersecurity controls and risk levels • Ensure that all cybersecurity risks remain at an acceptable level for the organisation's assets • Develop, maintain, report and communicate complete risk management cycle
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards • Analyse and consolidate organisation's quality and risk management practices • Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks • Enable employees to understand, embrace and follow the controls • Build a cybersecurity risk-aware environment • Communicate, present and report to relevant stakeholders • Propose and manage risk-sharing options
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Advanced knowledge of risk management frameworks, standards, methodologies, tools, guidelines and best practices • Knowledge of cyber threats, threats taxonomies and vulnerabilities repositories • Knowledge of risk sharing options and best practices • Knowledge of technical and organisational controls that appropriately mitigate cybersecurity risks • Knowledge of cybersecurity-related technologies and controls • Knowledge of monitoring, implementing, testing and evaluating the effectiveness of the controls

e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	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

2.11 DIGITAL FORENSICS INVESTIGATOR

Profile Title	**Digital Forensics Investigator**	
Alternative Title(s) *Lists titles under the same profile*	Digital Forensics Analyst Cybersecurity & Forensic Specialist Computer Forensics Consultant	
Summary statement *Indicates the main purpose of the profile.*	Ensure the cybercriminal investigation reveals all digital evidence to prove the malicious activity.	
Mission *Describes the rationale of the profile.*	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) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Digital Forensics Analysis	
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Develop digital forensics investigation policy, plans and procedures • Identify, recover, extract, document and analyse digital evidence • Preserve and protect digital evidence and make it available to authorised stakeholders • Inspect environments for evidence of unauthorised and unlawful actions • Systematically and deterministic document, report and present digital forensic analysis findings and results • Select and customise forensics testing, analysing and reporting techniques	
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Work ethically and independently; not influenced and biased by internal or external actors • Collect information while preserving its integrity • Identify, analyse and correlate events • Explain and present digital evidence in a simple, straightforward and easy to understand way • Develop and communicate, detailed and reasoned investigation reports	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of digital forensics methods, best practices and tools • Knowledge of digital forensics analysis techniques • Knowledge of digital forensics testing techniques • Knowledge of criminal investigation methodologies and procedures • Knowledge of malware analysis tools • Knowledge of cyber threats and vulnerabilities • Advanced knowledge of cybersecurity attacks tactics and techniques • Knowledge of legal framework related to cybersecurity and data protection • Knowledge of operating systems internals, networking protocols and services	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.7. Technology Trend Monitoring B.3. Testing B.5. Documentation Production E.3. Risk Management	Level 3 Level 4 Level 3 Level 3

2.12 PENETRATION TESTER

Profile Title	**Penetration Tester**	
Alternative Title(s) *Lists titles under the same profile*	Pentester Ethical Hacker Vulnerability Analyst Cybersecurity Tester Offensive Cybersecurity Expert Defensive Cybersecurity Expert Red Team Expert	
Summary statement *Indicates the main purpose of the profile.*	Assess the effectiveness of security controls, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors.	
Mission *Describes the rationale of the profile.*	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) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Technical Cybersecurity Assessment	
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Identify, analyse and assess technical and organisational cybersecurity vulnerabilities • Identify attack vectors, uncover and demonstrate exploitation of technical cybersecurity vulnerabilities • Test systems and operations compliance with regulatory standards • Select and develop appropriate penetration testing techniques • Organise test plans and procedures for penetration testing • Establish procedures for penetration testing result analysis and reporting • Document and report penetration testing results to stakeholders • Deploy penetration testing tools and test programs	
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Develop codes, scripts and programmes • Perform social engineering • Identify and exploit vulnerabilities • Conduct ethical hacking • Think creatively and outside the box • Solve and troubleshoot problems • Communicate and report • Use penetration testing tools effectively • Adapt and customise penetration testing tools and techniques	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Advanced knowledge of cybersecurity attack vectors • Advanced knowledge of IT/OT appliances, operating systems and computer networks • Advanced knowledge of penetration testing tools, techniques and methodologies • Knowledge of scripting and programming languages • Knowledge of security vulnerabilities • Knowledge of best practices on cybersecurity	
e-Competences (from e-CF)	B.2. Component Integration B.3. Testing	Level 4 Level 4

For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer	B.4. Solution Deployment B.5. Documentation Production E.3. Risk Management	Level 2 Level 3 Level 4

XX-00-00-000-XX-X

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 000-00-0000-000-0
doi: 0000.0000/000000