EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ECSF

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

SEPTEMBER 2022

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.

CONTACT

For contacting the editor please use euskills@enisa.europa.eu.

ACKNOWLEDGEMENTS

This framework is the result of the expert opinion and agreement in the Ad-Hoc Working Group on the skills framework composed by Agata BEKIER, Vladlena BENSON, Jutta BREYER*, Fabio DI FRANCO, Sara GARCIA, Athanasios GRAMMATOPOULOS, Markku KORKIAKOSKI, Csaba KRASZNAY, Haralambos MOURATIDIS, Christina GEORGHIADOU, Erwin ORYE*, Edmundas PIESARSKAS, Nineta POLEMI*, Paresh RATHOD*, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN and Jan HAJNY.

Fabio DI FRANCO and Athanasios GRAMMATOPOULOS led this activity for ENISA.

LEGAL NOTICE

COPYRIGHT NOTICE

* Rapporteur of Ad-Hoc Working Group on the European Cybersecurity Skills Framework

ISBN: 978-92-9204-584-5 – DOI: 10.2824/859537

TABLE OF CONTENTS

1. OVERVIEW

Chief Information Security Officer (CISO)

Cyber Incident Responder

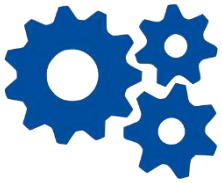
Cyber Legal, Policy and Compliance Officer

Cyber Threat Intelligence Specialist

Cybersecurity Architect

Cybersecurity Auditor

Cybersecurity Educator

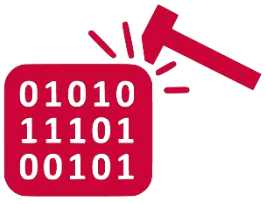


Cybersecurity Implementer

Cybersecurity Researcher

Cybersecurity Risk Manager

Digital Forensics Investigator



Penetration Tester

2. PROFILES

2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)

Profile Title	Chief Information Security Officer (CISO)
Alternative Title(s)	Cybersecurity Programme Director Information Security Officer (ISO) Information Security Manager Head of Information Security IT/ICT Security Officer
Summary statement	Manages an organisation's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected.
Mission	Defines, maintains and communicates the cybersecurity vision, strategy, policies and procedures. Manages the implementation of the cybersecurity policy across the organisation. Assures information exchange with external authorities and professional bodies.
Deliverable(s)	• Cybersecurity Strategy • Cybersecurity Policy
Main task(s)	• Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives • Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution • Supervise the application and improvement of the Information Security Management System (ISMS) • Educate senior management about cybersecurity risks, threats and their impact to the organisation • Ensure the senior management approves the cybersecurity risks of the organisation • Develop cybersecurity plans • Develop relationships with cybersecurity-related authorities and communities • Report cybersecurity incidents, risks, findings to the senior management • Monitor advancement in cybersecurity • Secure resources to implement the cybersecurity strategy • Negotiate the cybersecurity budget with the senior management • Ensure the organisation's resiliency to cyber incidents • Manage continuous capacity building within the organisation • Review, plan and allocate appropriate cybersecurity resources
Key skill(s)	• Assess and enhance an organisation's cybersecurity posture • Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks • Analyse and comply with cybersecurity-related laws, regulations and legislations • Implement cybersecurity recommendations and best practices • Manage cybersecurity resources • Develop, champion and lead the execution of a cybersecurity strategy • Influence an organisation's cybersecurity culture • Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Review and enhance security documents, reports, SLAs and ensure the security objectives • Identify and solve cybersecurity-related issues • Establish a cybersecurity plan • Communicate, coordinate and cooperate with internal and external stakeholders • Anticipate required changes to the organisation's information security strategy and formulate new plans

	• Define and apply maturity models for cybersecurity management • Anticipate cybersecurity threats, needs and upcoming challenges • Motivate and encourage people	
Key knowledge	• Cybersecurity policies • Cybersecurity standards, methodologies and frameworks • Cybersecurity recommendations and best practices • Cybersecurity related laws, regulations and legislations • Cybersecurity-related certifications • Ethical cybersecurity organisation requirements • Cybersecurity maturity models • Cybersecurity procedures • Resource management • Management practices • Risk management standards, methodologies and frameworks	
e-Competences (from e-CF)	A.7. Technology Trend Monitoring D.1. Information Security Strategy Development E.3. Risk Management E.8. Information Security Management E.9. IS-Governance	Level 4 Level 5 Level 4 Level 4 Level 5

2.2 CYBER INCIDENT RESPONDER

Profile Title	Cyber Incident Responder	
Alternative Title(s)	Cyber Incident Handler Cyber Crisis Expert Incident Response Engineer Security Operations Center (SOC) Analyst Cyber Fighter /Defender Security Operation Analyst (SOC Analyst) Cybersecurity SIEM Manager	
Summary statement	Monitor the organisation's cybersecurity state, handle incidents during cyber-attacks and assure the continued operations of ICT systems.	
Mission	Monitors and assesses systems' cybersecurity state. Analyses, evaluates and mitigates the impact of cybersecurity incidents. Identifies cyber incidents root causes and malicious actors. According to the organisation's Incident Response Plan, restores systems' and processes' functionalities to an operational state, collecting evidences and documenting actions taken.	
Deliverable(s)	• Incident Response Plan • Cyber Incident Report	
Main task(s)	• 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)	• Practice all technical, functional and operational aspects of cybersecurity incident handling and response • Collect, analyse and correlate cyber threat information originating from multiple sources • Work on operating systems, servers, clouds and relevant infrastructures • Work under pressure • Communicate, present and report to relevant stakeholders • Manage and analyse log files	
Key knowledge	• Incident handling standards, methodologies and frameworks • Incident handling recommendations and best practices • Incident handling tools • Incident handling communication procedures • Operating systems security • Computer networks security • Cyber threats • Cybersecurity attack procedures • Computer systems vulnerabilities • Cybersecurity-related certifications • Cybersecurity related laws, regulations and legislations • Secure Operation Centres (SOCs) operation • Computer Security Incident Response Teams (CSIRTs) operation	
e-Competences (from e-CF)	A.7. Technology Trend Monitoring B.2. Component Integration	Level 3 Level 2

	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)	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 frameworks based on the organisation's strategy and legal requirements.
Mission	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 and recommended remediation strategies/solutions to ensure compliance.
Deliverable(s)	• Compliance Manual • Compliance Report
Main task(s)	• Ensure compliance with and provide legal advice and guidance on data privacy and data protection standards, laws and regulations • Identify and document compliance gaps • 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 • Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization • Manage legal aspects of information security responsibilities and third-party relations
Key skill(s)	• Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' 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 • 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 • 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 • Collaborate with other team members and colleagues
Key knowledge	• Cybersecurity related laws, regulations and legislations

	• Cybersecurity standards, methodologies and frameworks • Cybersecurity policies • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Privacy impact assessment standards, methodologies and frameworks	
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

2.4 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 by cyber threat actors and their trends, track threat actors' activities and observe how non-cyber events can influence cyber-related actions.
Deliverable(s)	• Cyber Threat Intelligence Manual • Cyber Threat Report
Main task(s)	• 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)	• Collaborate with other team members and colleagues • 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 • Communicate, coordinate and cooperate with internal and external stakeholders • Communicate, present and report to relevant stakeholders • Use and apply CTI platforms and tools
Key knowledge	• Operating systems security • Computer networks security • Cybersecurity controls and solutions • Computer programming • Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks • Responsible information disclosure procedures • Cross-domain and border-domain knowledge related to cybersecurity • Cyber threats • Cyber threat actors • Cybersecurity attack procedures • Advanced and persistent cyber threats (APT) • Threat actors Tactics, Techniques and Procedures (TTPs) • Cybersecurity-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

2.5 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)	• Cybersecurity Architecture Diagram • Cybersecurity Requirements Report
Main task(s)	• 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)	• Conduct user and business security requirements analysis • Draw cybersecurity architectural and functional specifications • Decompose and analyse systems to develop security and privacy requirements and identify effective solutions • 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 • Communicate, present and report to relevant 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 • Coordinate the integration of security solutions
Key knowledge	• Cybersecurity-related certifications • Cybersecurity recommendations and best practices • Cybersecurity standards, methodologies and frameworks • Cybersecurity-related requirements analysis • Secure development lifecycle • Security architecture reference models • Cybersecurity-related technologies • Cybersecurity controls and solutions • Cybersecurity risks • Cyber threats • Cybersecurity trends • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Legacy cybersecurity procedures • Privacy-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

2.6 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	Perform cybersecurity audits on the organisation's ecosystem. 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)	• Cybersecurity Audit Plan • Cybersecurity Audit Report	
Main task(s)	• 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 • Monitor risk remediation activities	
Key skill(s)	• 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 • Decompose and analyse systems to identify weaknesses and ineffective controls • Communicate, explain and adapt legal and regulatory requirements and business needs • Collect, evaluate, maintain and protect auditing information • Audit with integrity, being impartial and independent	
Key knowledge	• Cybersecurity controls and solutions • Legal, regulatory and legislative compliance requirements, recommendations and best practices • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Conformity assessment standards, methodologies and frameworks • Auditing standards, methodologies and frameworks • Cybersecurity standards, methodologies and frameworks • Auditing-related certification • Cybersecurity-related certifications	
e-Competences (from e-CF)	B.3. Testing B.5. Documentation Production E.3. Risk Management E.6 ICT Quality Management	Level 4 Level 3 Level 4 Level 4

	E.8. Information Security Management	Level 4

2.7 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)	• Cybersecurity Awareness Program • Cybersecurity Training Material	
Main task(s)	• 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)	• Identify needs in cybersecurity awareness, training and education • Design, develop and deliver learning programmes to cover cybersecurity needs • Develop cybersecurity exercises including simulations using cyber range environments • Provide training towards cybersecurity and data protection professional certifications • Utilise existing cybersecurity-related training resources • Develop evaluation programs for the awareness, training and education activities • Communicate, present and report to relevant stakeholders • Identify and select appropriate pedagogical approaches for the intended audience • Motivate and encourage people	
Key knowledge	• Pedagogical standards, methodologies and frameworks • Cybersecurity awareness, education and training programme development • Cybersecurity-related certifications • Cybersecurity education and training standards, methodologies and frameworks • Cybersecurity related laws, regulations and legislations • Cybersecurity recommendations and best practices • Cybersecurity standards, methodologies and frameworks • Cybersecurity controls and solutions	
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

2.8 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 organisation's cybersecurity-related solutions (systems, assets, software, controls and services), infrastructures and products.	
Deliverable(s)	• Cybersecurity Solutions	
Main task(s)	• 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)	• Communicate, present and report to relevant 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 code, scripts and programmes • Identify and solve cybersecurity-related issues • Collaborate with other team members and colleagues	
Key knowledge	• Secure development lifecycle • Computer programming • Operating systems security • Computer networks security • Cybersecurity controls and solutions • Offensive and defensive security practices • Secure coding recommendations and best practices • Cybersecurity recommendations and best practices • Testing standards, methodologies and frameworks • Testing procedures • Cybersecurity-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

2.9 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)	• Publication in Cybersecurity	
Main task(s)	• 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)	• Generate new ideas and transfer theory into practice • Decompose and analyse systems to identify weaknesses and ineffective controls • Decompose and analyse systems to develop security and privacy requirements and identify effective solutions • Monitor new advancements in cybersecurity-related technologies • Communicate, present and report to relevant stakeholders • Identify and solve cybersecurity-related issues • Collaborate with other team members and colleagues	
Key knowledge	• Cybersecurity-related research, development and innovation (RDI) • Cybersecurity standards, methodologies and frameworks • Legal, regulatory and legislative requirements on releasing or using cybersecurity related technologies • Multidiscipline aspect of cybersecurity • Responsible information disclosure procedures	
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

2.10 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-related risks aligned to the organisation's 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 Assessment Report • Cybersecurity Risk Remediation Action Plan	
Main task(s)	• 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)	• 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 • Build a cybersecurity risk-aware environment • Communicate, present and report to relevant stakeholders • Propose and manage risk-sharing options	
Key knowledge	• Risk management standards, methodologies and frameworks • Risk management tools • Risk management recommendations and best practices • Cyber threats • Computer systems vulnerabilities • Cybersecurity controls and solutions • Cybersecurity risks • Monitoring, testing and evaluating cybersecurity controls' effectiveness • Cybersecurity-related certifications • Cybersecurity-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

2.11 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)	• Digital Forensics Analysis Results • Electronic Evidence	
Main task(s)	• 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)	• Work ethically and independently; not influenced and biased by internal or external actors • Collect information while preserving its integrity • Identify, analyse and correlate cybersecurity 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	• Digital forensics recommendations and best practices • Digital forensics standards, methodologies and frameworks • Digital forensics analysis procedures • Testing procedures • Criminal investigation procedures, standards, methodologies and frameworks • Cybersecurity related laws, regulations and legislations • Malware analysis tools • Cyber threats • Computer systems vulnerabilities • Cybersecurity attack procedures • Operating systems security • Computer networks security • Cybersecurity-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

2.12 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)	• Vulnerability Assessment Results Report • Penetration Testing Report	
Main task(s)	• 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)	• Develop codes, scripts and programmes • Perform social engineering • Identify and exploit vulnerabilities • Conduct ethical hacking • Think creatively and outside the box • Identify and solve cybersecurity-related issues • Communicate, present and report to relevant stakeholders • Use penetration testing tools effectively • Conduct technical analysis and reporting • Decompose and analyse systems to identify weaknesses and ineffective controls • Review codes assess their security	
Key knowledge	• Cybersecurity attack procedures • Information technology (IT) and operational technology (OT) appliances • Offensive and defensive security procedures • Operating systems security • Computer networks security • Penetration testing procedures • Penetration testing standards, methodologies and frameworks • Penetration testing tools • Computer programming • Computer systems vulnerabilities • Cybersecurity recommendations and best practices • Cybersecurity-related certifications	
e-Competences (from e-CF)	B.2. Component Integration B.3. Testing B.4. Solution Deployment B.5. Documentation Production	Level 4 Level 4 Level 2 Level 3

	E.3. Risk Management	Level 4

3. DELIVERABLES LIBRARY

The list of deliverables provides some indicative and practical examples of the deliverable(s) / output(s) of each role profile. The deliverables listed are offered as examples as the list is not exhaustive, and thus mat not cover every aspect of each profile.

Profile Title	Deliverable	Description
Chief Information Security Officer (CISO)	Cybersecurity Strategy	Cybersecurity Strategy is a plan of actions designed to improve the security and resilience of an organisation's infrastructures and services.
Chief Information Security Officer (CISO)	Cybersecurity Policy	A policy listing rules to ensure the organisation's cybersecurity.
Cyber Incident Responder	Incident Response Plan	A set of documented procedures detailing the steps that should be taken in each phase of an incident response (Preparation, Detection and Analysis, Containment, Eradication and Recovery, Post-Incident Activity).
Cyber Incident Responder	Cyber Incident Report	A report providing details on one or more cyber incidents.
Cyber Legal, Policy & Compliance Officer	Compliance Manual	A manual providing a thorough understanding of the regulatory compliance obligations of an organisation. It may include internal policies or procedures to ensure compliance with laws, regulations and/or standards.
Cyber Legal, Policy & Compliance Officer	Compliance Report	A report presenting the current state of the compliance posture of an organisation.
Cyber Threat Intelligence Specialist	Cyber Threat Intelligence Manual (or Handbook)	A manual presenting tools and/or methodologies for cyber threat intelligence gathering and/or sharing.
Cyber Threat Intelligence Specialist	Cyber Threat Report	A report identifying prime threats, major trends observed with respect to threats, threat actors and/or attack techniques. The report may also include relevant mitigation measures.
Cybersecurity Architect	Cybersecurity Architecture Diagram	A visual representation of an organisation's cybersecurity system architecture used to protect assets against cyber-attacks.
Cybersecurity Architect	Cybersecurity Requirements Report	A report listing a set of requirements needed for ensuring the cybersecurity of a system.
Cybersecurity Auditor	Cybersecurity Audit Plan	A plan that presents the overall strategy and the procedures an auditor will follow to conduct a cybersecurity audit.
Cybersecurity Auditor	Cybersecurity Audit Report	A report providing a thorough understanding of the level of security of a system, assessing its cybersecurity strengths and weaknesses. It may also provide remediation actions to improve the overall cybersecurity of the system.
Cybersecurity Educator	Cybersecurity Awareness Program	A program of activities to raise awareness on cybersecurity-related issues (e.g. lectures on attacks

		and threats) helping organisations prevent and mitigate related cybersecurity risks.
Cybersecurity Educator	Cybersecurity Training Material	Material providing explaining cybersecurity-related concepts, methodologies and tools for training or upskilling individuals. It might include Handbooks for teachers, Toolsets for students and/or Virtual Images to support hands on training sessions.
Cybersecurity Implementer	Cybersecurity Solutions	Cybersecurity solutions might include tools and services that aim to protect organizations against cyber-attacks.
Cybersecurity Researcher	Publication in Cybersecurity	Academic publication releasing findings and results of research in the cybersecurity context. The purpose of the publication might be to advance the technology and/or develop new innovated solutions.
Cybersecurity Risk Manager	Cybersecurity Risk Assessment Report	A report listing the results of the identification, analysis, and evaluation of cybersecurity risks of a system. It might also include controls to mitigate or reduce identified risks to an acceptable level.
Cybersecurity Risk Manager	Cybersecurity Risk Remediation Action Plan	An action plan listing activities related to the implementation of mitigation measures aiming at reducing cybersecurity risks.
Digital Forensics Investigator	Digital Forensics Analysis Results	Results of the analysis of digital data uncovering potential evidence of malicious incidents and identifying possible threat actors.
Digital Forensics Investigator	Electronic Evidence	Potential evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network. (e.g. accurate collection of logs)
Penetration Tester	Vulnerability Assessment Results Report	A report listing and assessing the criticality of vulnerabilities uncovered in a system during a (usually automatic) vulnerability scanning. The report might also suggest basic remediation actions.
Penetration Tester	Penetration Testing Report	A report providing a detailed and comprehensive analysis of a system's vulnerabilities identified during a security testing. The report might also include suggested remediation actions.

TP-09-22-510-EN-N

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: 978-92-9204-584-5
DOI: 10.2824/859537