DIGITAL4Security Needs Analysis Report

D.2.1

Digital4Security
Shaping Europe's cyber future

Table of Contents

1. ABOUT THE DIGITAL4Security PROJECT

Digital4Security is a ground-breaking pan-European master's programme aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. With funding of almost 20 million euros from the European Union, this four-year initiative has garnered support from a Consortium comprising 31 partners spanning 14 countries. This industry-driven programme will provide comprehensive knowledge of cybersecurity management, regulatory compliance, and technical expertise to European SMEs and companies.

2. The DIGITAL4Security CONSORTIUM

The DIGITAL4Security Consortium is a dynamic pan-European partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management programme, developed and delivered by the best cybersecurity talent from Europe and worldwide.

Partners	Acronym
NATIONAL UNIVERSITY OF SCIENCE AND TEHNOLOGY POLITEHNICA BUCHAREST	Politehnica Bucharest
SCHUMAN ASSOCIATES SCRL	SA
ATAYA & PARTNERS	ATAYA
POLITECNICO DI MILANO	POLIMI
POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	CMIP
CONTRADER SRL	CONTRADER
DIGITAL TECHNOLOGY SKILLS LIMITED	DTSL
INDEPENDENT PICTURES LIMITED	Indiepics
MATRIX INTERNET APPLICATIONS LIMITED	MATRIX
PROFIL KLETT D.O.O.	PROFIL KLETT
SERVICENOW IRELAND LIMITED	ServiceNow

UNIVERSITA DEGLI STUDI DI BRESCIA	UNIBS
UNIVERSITY OF DIGITAL SCIENCE GGMBH	UDS
SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	SKILLNET
IT@CORK ASSOCIATION LIMITED LBG	IT@CORK
ADECCO FORMAZIONE SRL	ADECCO TRAINING
UNIVERSITAT KOBLENZ	UNI KO
VYSOKE UCENI TECHNICKE V BRNE	BRNO UNIVERSITY
MUNSTER TECHNOLOGICAL UNIVERSITY	MTU
EUROPEAN DIGITAL SME ALLIANCE	DIGITAL SME
DIGITALEUROPE AISBL	DIGITALEUROPE
MYKOLO ROMERIO UNIVERSITETAS	MRU
SVEUCILISTE U RIJECI	UNIRI
NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	NASK
UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA	UNIR
NATIONAL COLLEGE OF IRELAND	NCI
TERAWE TECHNOLOGIES LIMITED	TERAWE
CY CERGY PARIS UNIVERSITE	CY CERGY PARIS
BANCO SANTANDER SA	BANCO SANTANDER
CYBER RANGES LTD	SILENSEC
RED OPEN S.R.L.	RED OPEN S.R.L.
VYTAUTO DIDZIOJO UNIVERSITETA	VMU

Associated Partners	Acronym
FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	FHG
Pearson Benelux BV	Pearson Benelux
AGORIA ASBL	AGORIA ASBL

Document Control Information

Project	Digital4Security
Document Title	DIGITAL4Security Needs Analysis Report
Work Package Number	WP2
Deliverable Number	D2.1
Lead Beneficiary	DTSL
Project Coordinator:	National University of Science and Technology Politehnica of Bucharest (NUSTPB)
Dissemination Level	**Sensitive** — limited under the conditions of the Grant Agreement
Authors	Carmel Somers (DTSL)
Reviewers	Reviewers (DTSL) 1st level review (MTU) 2nd level review (UPB) final review
Description	The aim of the DIGITAL4Security Needs Analysis is to gain an understanding of the skills and knowledge areas needed for the ECSF roles on which the Master's programme will be based.
Status	Draft
Delivery Date	26.02.2024
Due date	26.02.2024
Approval Date:	DD.MM.YYYY

Revision history

Version	Date	Modified by	Comments
1	07.02.2024	Carmel Somers	Initial Draft
2	16.02.2024	Carmel Somers	Following Review by MTU
3	01.03.2024	Ciprian-Mihai Dobre (UNSTPB)	Initial public review

3. EXECUTIVE SUMMARY

The objective of conducting the skills needs analysis for cybersecurity roles is to identify and map the requisite competencies against the evolving threat landscape ensuring that cybersecurity professionals are equipped to meet current and future challenges. Aligning this analysis with the European Union Agency for Cybersecurity (ENISA) European Cybersecurity Skills Framework (ECSF) is crucial, as it ensures that the identified skills are standardised, comprehensive, and in line with European best practices. This alignment not only facilitates a structured approach to workforce development but also enhances mutual recognition of skills across member states. The outcome of such a tailored analysis is expected to significantly bolster an organisation's cybersecurity posture and strategy, leading to a more resilient infrastructure, informed risk management, and an overall strengthened defence against cyber threats.

The *European Cybersecurity Skills Framework (ECSF)*, (2022) contains twelve cybersecurity role profiles defined by the framework to provide a common understanding of the main cybersecurity missions, tasks, and skills needed in a professional cybersecurity context. As such it is a valuable reference for profiling skills and knowledge needed by cybersecurity professionals.

The framework was designed to be understood and comprehensive enough to provide appropriate in-depth cybersecurity insights in addition to supporting customisation based on each user's needs. By incorporating all stakeholder perspectives, the framework is applicable to all types of organisations and supports the development of all cybersecurity professions.

The "Cybersecurity Needs Analysis Report" for the DIGITAL4Security project outlines the comprehensive needs for a European Cybersecurity Masters Programme. The report emphasises the importance of aligning with the ENISA European Cybersecurity Skills Framework (ECSF) to ensure standardised, comprehensive skill sets that meet current and future cybersecurity challenges. Key findings from the analysis reveal a robust foundation of established cybersecurity skills, with a substantial addition of new knowledge areas and skills reflecting the field's dynamic evolution. There is a particular emphasis on communication, creativity, technical proficiency, integrity, and information analysis.

The recommended actions for academia include integrating frequently mentioned knowledge areas and skills into the curriculum, emphasising multidisciplinary knowledge that spans technical, legal, regulatory, and ethical aspects. This approach ensures that students' gain a holistic understanding of cybersecurity, enabling them to navigate complex challenges effectively.

Practical skills development should be a central focus of cybersecurity education. Skills including legal and compliance training, risk management and an understanding of regulatory frameworks and the development of soft skills are highlighted as crucial educational components. An emphasis on risk management techniques equips students' with the ability to assess and mitigate cybersecurity risks proactively.

Curricula design should prioritise the integration of both technical and soft skills development. By incorporating elements such as critical thinking, communication and adaptability, academia can produce well-rounded cybersecurity professionals capable of addressing the dynamic nature of cyber threats. This holistic approach aims to bridge the cybersecurity skills gap and revolutionise cybersecurity education within Europe, ultimately enhancing security measures against intensifying cyber threats.

4. INTRODUCTION

In an era where digital security is paramount, the DIGITAL4Security project emerges as a pivotal initiative, directly addressing four critical key objectives:

(1) addressing skills needs,
(2) attracting qualified teaching staff and students,
(3) upgrading digital solutions, equipment and infrastructure and
(4) establishing structural and sustainable partnerships.

This report presents a comprehensive needs analysis for the DIGITAL4Security programme, and is a key deliverable of Work Package 2 (Task 2.1). The overall goal of the project is to

create a robust educational framework that not only bridges the growing cybersecurity skills gap but also revolutionises how cybersecurity education is delivered and applied in the European context.

The paramount goal of the DIGITAL4Security initiative is the establishment of a Master's Programme in Cybersecurity Management that is characterised by its high level of innovation, efficacy, and sustainability. This academic endeavour is designed to produce a consistent output of skilled experts in cybersecurity management, individuals who will be essential in fortifying the security framework of European industrial and public sectors in the face of intensifying cyber threats.

In pursuit of this objective, the programme aspires to foster an environment of inclusivity that appeals to a broad spectrum of students and corporate entities. With an ambitious aim to educate and mentor over 2500 students within a span of four years, the programme is committed to not only imparting theoretical knowledge but also providing practical, industry-relevant experiences and mentorship.

A pivotal component of this venture is the implementation of a shared, cloud-based Digital Learning Platform, which aims to revolutionise the educational landscape. This advanced platform is envisioned to become the cornerstone of the Master's programme, offering a digital nexus that connects all consortium partners including Higher Education Institutions, training providers, research entities, and industrial collaborators. This integration will enable an unprecedented level of secure interoperability among the IT systems of the participating organisations.

Moreover, the programme aims to lay the foundation for a robust European Stakeholder Network. This network is expected to catalyse a dynamic and mutually beneficial partnership among the academic partners, the cybersecurity industry, research institutions, and employment sectors. The strategy is to undertake extensive capacity building and training for the universities and training organisations that are part of this initiative. Leveraging the specialised knowledge housed within the consortium and its extended network of industry and academic partners, the programme seeks to establish lasting connections that bridge the gap between academic cybersecurity studies and industry application.

DIGITAL4Security's master programme will be tailored to meet the needs of European companies across multiple sectors, ranging from SMEs to large corporates. Special emphasis will be placed on businesses engaged in Smart Technologies and Systems, and those managing data that may be highly coveted by cybercriminals.

This report delves into the specifics of these objectives, seeking to understand the roles, knowledge and skills needed by individuals seeking employment in one of the ENISA ECSF Role profiles. This master's programme aims to address their skills needs through a programme that not only educates but empowers, fostering a new generation of cybersecurity experts equipped to navigate and mitigate the complexities of the digital age.

5. ENISA ECSF ROLE PROFILES

The DIGITAL4Security Master's programme is structured around seven key roles identified in ENISA's ECSF Framework. These roles encompass a spectrum of expertise within the cybersecurity domain, including strategic leadership, threat analysis, educational outreach, investigative proficiency, audit and compliance, risk management, and legal advisory. Each role plays a role in building a robust defence against the growing landscape of cyber threats and ensuring the security and compliance of organisational IT infrastructures.

1. **Chief Information Security Officer (CISO):** A CISO is responsible for setting the organisation's cybersecurity strategy and leading the IT security department. They ensure that information assets and technologies are adequately protected, aligning security initiatives with business objectives.
2. **Cyber Threat Intelligence Specialist:** This role involves analysing and interpreting information about potential threats to proactively defend against cyber-attacks. Specialists gather intelligence from various sources to anticipate and mitigate cyber threats.
3. **Cybersecurity Educator**: A Cybersecurity Educator designs and delivers educational programmes and courses in cybersecurity. They are responsible for raising awareness and understanding of cybersecurity principles among students or organisational staff.
4. **Digital Forensics Investigator**: Digital Forensics Investigators specialise in uncovering and analysing electronic data to solve cybercrimes. They recover and

investigate material found in digital devices, often in the context of legal proceedings.

5. **Cybersecurity Auditor**: Cybersecurity Auditors examine and evaluate an organisation's IT infrastructure to ensure security policies, controls, and practices comply with regulatory and internal standards. They identify vulnerabilities and suggest improvements.
6. **Cybersecurity Risk Manager**: This role focuses on identifying, evaluating, and providing risk response strategies to mitigate cybersecurity threats. They play a crucial part in the organisation's risk management framework.
7. **Cyber Legal, Policy, & Compliance Officer**: Officers in this role advise on legal and regulatory requirements related to cybersecurity. They ensure that the organisation complies with cybersecurity laws, policies, and standards, and they help navigate legal implications of digital security measures.

6. METHODOLOGY

The methodology for the Needs Analysis encapsulates three principal activities: a collaborative review of the ENISA ECSF role profiles by academic and industry partners to identify knowledge and skills gaps, an online survey aimed at pinpointing the essential skills and knowledge required for the master's target audience, and a thorough examination of current research and publications related to cybersecurity skills, knowledge areas, and the ECSF role profiles. In the ENISA ECSF Framework), "Knowledge Areas" and "Skills" are foundational components designed to systematically categorise and define the expertise required in the cybersecurity domain. Knowledge Areas refer to broad domains of expertise, encompassing specific sets of concepts, theories, principles, and practices essential for cybersecurity professionals. These areas cover a wide spectrum of topics, from risk management to cybersecurity defence, providing a structured overview of the theoretical and conceptual background needed in the field. On the other hand, "Skills" within the ECSF are focused on the practical application of this knowledge, detailing the ability to perform tasks and solve problems. Skills are outlined as specific competencies, both technical and non-technical, that are necessary to effectively carry out roles and responsibilities in cybersecurity. Together, these components of the ECSF create a comprehensive framework that helps in identifying and developing the necessary competencies for professionals in the cybersecurity

workforce, aiming to align educational and training programs with industry needs, facilitate career development, and streamline recruitment processes.

6.1 Academic & Industry Partner Review of the 12 ECSF Profiles

The methodology for the DIGITAL4Security project commenced with an academic review of the ECSF Profiles. The objective was to establish a foundational understanding of the knowledge areas and skills outlined in the 12 ECSF profiles: "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", and "Penetration Tester".

It further sought to add context to the existing knowledge areas and skills. As the ECSF did not prioritise the knowledge areas or skills in their framework, the review undertook to prioritise these using a rating system where “Priority 1” represented a low priority and “Priority 5” represented a high priority designation. The reviewers were also asked to identify any existing ECSF knowledge areas or skills they believed should be added to other roles in the framework. If they determined knowledge areas or skills not already in the ECSF framework were needed for the role profiles they should add these as they conducted their review. To achieve this, excel spreadsheets containing two ECSF roles, their skills and knowledge areas and associated categories were shared with six pairs of academic partners for their review, covering all 12 profiles. On conclusion of an extensive academic review, enhanced knowledge and skills descriptors were applied for greater clarity, and both knowledge areas and skills were prioritised in order of importance and additional skills and knowledge areas needed for the ECSF role profiles were added.

Following the academic review, six Industry partners in the consortium evaluated the outcome of the academic partner’s review. They conducted a similar review and agreed or challenged the prioritisation and worked with the academic partners to agree the final knowledge areas and skills. The industry partners also identified additional knowledge and skills needed based on their awareness of the cybersecurity skills needs in the marketplace.

On completion of the industry review the excel sheets were consolidated into two sheets – one containing the cybersecurity skills and one containing the knowledge areas. The columns in each sheet contained the ECSF profiles and the rows contained the skills or knowledge area descriptors, the categories to which they belong and the designated priority level of each. The presence of a skill which existed in the ENISA ECSF framework was marked in the column of the role it applies to with a black "**X**", indicating the relevance or requirement of that skill for the role. For example, the skill "*Collect, analyse and correlate cyber threat information originating from multiple sources"* in the "Threat Analysis" category was marked as relevant for the role of Cyber Auditor. A red "**X**" indicated that this skill which existed in the ENISA ECSF framework, was identified during the review process as a skill that should also apply to the Cyber Legal, Policy & Compliance Officer role as seen in Figure 1 below.

Original ENISA Skill Description	ENISA Skill Description with added Context	Category	CISO	Cyber Legal, Policy & Compliance Officer	Cyber Threat Intelligence Specialist	Cybersecurity Auditor
Collect, analyse and correlate cyber threat information originating from multiple sources	Possess expertise in assessing information security effectiveness, identifying risk exposures, and protect the availability, confidentiality and audit trails of information from destruction or manipulation.	Threat Analysis		X		X
Collect, evaluate, maintain and protect auditing information	Skills in collecting, evaluating, maintaining, and protecting auditing information. This includes attention to the confidentiality and integrity of audit data.	Information Security Controls Assessment			X	X

Figure 1: Example of a skill aligned to Role Profiles

This consolidation aids in determining the most sought-after skills in cybersecurity roles, pinpointing skill shortages, and will help shape relevant training programmes. It also clarifies the classification and importance of diverse skills in the field of cybersecurity. The ENISA ECSF framework has 78 unique skills which are employed to varying degrees across the 12 ECSF profiles. The framework has multiple categories, the addition of new categories such as "Collaboration / Communication" as outlined in Figure 2 below, and the indication of skills

and category applicability to different roles provides a more detailed and role-specific approach to categorising the existing ECSF skills and newly identified skills.

Original ENISA Skill Description	ENISA Skill Description with added Context	Category	CISO	Cyber Legal, Policy & Compliance Officer	Cyber Threat Intelligence Specialist	Cybersecurity Auditor
Collaborate with other team members and colleagues	Effective communication and collaboration, involving the sharing of information, understanding of risks, and adherence to standards. Skilled in conveying ideas, active listening, understanding diverse perspectives, mediating discussions, and negotiating solutions. Maintaining composure under pressure, being adaptable, reliable, and respectful are critical to fostering positive team dynamics and building cross-functional, human-centric teams that can respond to and manage cybersecurity challenges effectively.	Collaboration / Communication		X	X	X
Collect, analyse and correlate cyber threat information originating from multiple sources	Possess expertise in assessing information security effectiveness, identifying risk exposures, and protect the availability, confidentiality and audit trails of information from destruction or manipulation.	Threat Analysis		X		X
Collect, evaluate, maintain and protect auditing information	Skills in collecting, evaluating, maintaining, and protecting auditing information. This includes attention to the confidentiality and integrity of audit data.	Information Security Controls Assessment			X	X

Figure 2: Consolidated View – Skills aligned to ECSF Roles

The consolidation of the knowledge areas across the 12 ECSF role profiles followed the same process. The ENISA ECSF framework has 67 unique knowledge areas which are associated with the 12 ECSF profiles. The knowledge areas are categorised, prioritised and contain the addition of new knowledge areas and in some cases new categories were defined during the review.

The outcome is a consolidated unified framework outlining the essential knowledge areas and skills for each ECSF profile, informed by both academic theory and industry practice. The framework will be shared with the ENISA ECSF working group for their consideration and are included in the appendices of this document.

6.2 Online Survey

The DIGITAL4Security project was designed to focus on 7 of the 12 ECSF role profiles (Chief Information Security Officer (CISO), Cyber Threat Intelligence Specialist, Cybersecurity Educator, Digital Forensics Investigator, Cybersecurity Auditor, Cybersecurity Risk Manager and Cyber Legal, Policy, & Compliance Officer). The development and review of survey questions based on these 7 roles was conducted with the objective to gather targeted insights from a broader audience of the in demand cybersecurity knowledge areas and skills. In addition, it sought to gather perspectives on the development and delivery of the master's programme. The other objective was to understand the cybersecurity concerns of those organisations working with smart technologies and systems and/or those managing sensitive data which might be of specific interest to cyber criminals.

A set of survey questions was developed based on the consolidated profile reviews and the DIGITAL4Security project goals as set out in DIGITAL4Security project documentation. The questions were reviewed by a number of the consortium partners and refined to ensure relevance and clarity. The outcome is a finalised set of survey questions published in Survey Monkey, an online survey tool and distributed by each partner via a link in specifically targeted emails and in a broader dissemination through partner social media networks and marketing materials. Each partner was provided with an email template and a social media template to ensure the consistency of the messaging when the survey link was disseminated. This broad distribution aimed to reach a diverse range of respondents across different sectors and geographical locations. The outcome was a rich dataset providing insights into the current state of cybersecurity skills and industry expectations which will feed into the development of the master's programme.

6.3 Review of Existing Research & Publications

The industry and academic consortium partners provided examples of recent cybersecurity reports focused on cybersecurity skills related to the ECSF roles on which the master's programme will be based. The methodology for reviewing cybersecurity reports, publications and research was multifaceted, beginning with the collection of materials from trusted industry, academic, and government sources. These documents were sorted based on their relevance to the 7 ECSF roles. A detailed content analysis was then undertaken to extract

pertinent data on the required skills and knowledge areas. This analysis was cross-referenced with the ECSF competencies to identify potential alignment.

7. SKILLS AND KNOWLEDGE GAP ANALYSIS

7.1 Analysis of the Academic & Industry Review of the ECSF Skills

The ENISA ECSF framework lists 78 different skills spread across 12 job roles, showing a wide range of abilities specific to each role. A review by academic and industry experts identified 6 skills that were not in the ENISA framework. These skills are proposed to be included for the Chief Information Security Officer (CISO) role (1 skill - Stakeholder Management) and the Cyber Threat Intelligence Specialist role (5 skills – Change Management; Certifications; Technical Proficiency; Incident Response Processes & Procedures; Continuous Learning). Furthermore, the review suggested adding certain skills already in the ENISA framework to other roles in the framework. For this analysis, any existing ENISA skills that are proposed to be added to other roles are considered "new" skills for those roles. These are in addition to the 6 newly identified skills.

Table 1 presents the number of cybersecurity skills associated with each role according to the ECSF framework. It also shows the total number of skills recommended for each role after a recent review. The column labelled "New" indicates skills that have been added to the roles as a result of this review. The rest of the columns classify these skills by their level of importance, with Priority 5 being the highest and Priority 1 being the lowest.

For the CISO role, originally 14 skills were specified by the ECSF. After the review, 8 additional skills are recommended to be included for this role. Out of these, 1 skill is completely new to the ECSF framework, while the other 7 are pre-existing within the framework.

As for the Penetration Tester role, it had 11 skills listed in the original ECSF framework. The review suggested adding 10 more skills from the ECSF list to this role.

Role	Cybersecurity Skills by Priority							
	ECSF Total	Total	New	Priority 5	Priority 4	Priority 3	Priority 2	Priority 1
CISO	14	22	8	7	12	3	0	0
Penetration Tester	11	21	10	3	14	4	0	0
Cyber Incident Responder	6	9	3	4	4	0	1	0
Cyber Legal Policy & Compliance Officer	8	8	0	4	3	1	0	0
Cyber Threat Intelligence Specialist	10	27	17	7	13	2	4	1
Cybersecurity Architect	10	21	11	5	15	1	0	0
Cybersecurity Auditor	7	15	8	5	8	2	0	0
Cybersecurity Educator	10	10	0	0	7	2	1	0
Cybersecurity Researcher	7	12	5	1	4	2	5	0
Digital Forensics Investigator	5	12	7	2	3	4	2	1
Cybersecurity Implementor	7	11	4	1	10	0	0	0
Cybersecurity Risk Manager	5	5	0	2	1	1	1	0

Table 1: Cybersecurity Skills by Role by Priority

Across various cybersecurity role profiles, the top 10 new skills identified in the ENISA skills list that emerge with the highest frequency include *effective communication with stakeholders* and *creative thinking*, both occurring four times. Skills in *integrating cybersecurity solutions into organisational infrastructure, monitoring technological advancements, anticipating future threats and challenges,* and *assessing solution performance* each appear three times. Additionally, the *ability to conduct impartial and independent audits*, *collaborate with teammates*, *analyse threat information from diverse sources*, and *manage auditing information* are noted twice, reflecting the evolving landscape of cybersecurity competencies.

These skills emphasise a range of competencies, including communication, creativity, technical proficiency, integrity, collaboration, and information analysis in the cybersecurity field

The identification of these 10 skills as new and needed across the ECSF role profiles suggests several key insights about the evolving landscape of cybersecurity and the competencies required to navigate it effectively:

1. **Emphasis on Communication and Collaboration**: The frequent mention of skills like "*Communicate, coordinate and cooperate with internal and external stakeholders*" and "*Collaborate with other team members and colleagues*" highlights the growing importance of interpersonal skills in cybersecurity. This trend indicates that cybersecurity is increasingly seen as a collaborative field, requiring professionals to work effectively with diverse teams and stakeholders.
2. **Need for Creativity and Innovation**: The skill "*Think creatively and outside the box*" being identified as a new requirement suggests that the field is evolving beyond traditional, formulaic approaches. This reflects a recognition that cybersecurity challenges are becoming more complex and diverse, necessitating innovative problem-solving approaches.
3. **Integration of Cybersecurity Solutions**: The importance of "*Integrating cybersecurity solutions into existing infrastructures*" indicates a shift towards a more holistic approach to cybersecurity. It shows the need for professionals who can not only understand technical aspects but also implement these solutions seamlessly within organisational contexts.
4. **Staying Current with Technological Advancements**: Skills like "*Monitor new advancements in cybersecurity-related technologies*" underscore the rapid pace of technological change in this field. Professionals are expected to continuously update their knowledge and adapt to new tools, techniques, and threats.
5. **Proactive Threat Management**: The skill "*Anticipate cybersecurity threats, needs and upcoming challenges*" suggests a move towards a more proactive stance in cybersecurity. Rather than reacting to incidents, there is a growing focus on predicting and preventing potential threats.
6. **Focus on Security and Performance Assessment**: The inclusion of "*Assess the security and performance of solutions*" reflects the dual focus on not only ensuring security but also maintaining system performance. This balance is critical in a world where efficiency and security are both key.

7. **Integrity in Auditing**: "*Audit with Integrity, being impartial and independent*" indicates a heightened emphasis on ethics and responsibility in cybersecurity roles, particularly in positions of trust and authority.
8. **Collaborating with teammates**: Working effectively with others within a cybersecurity team to address and solve security issues.
9. **Enhanced Information Analysis**: Skills related to the collection and analysis of cyber threat information highlight the increasing importance of data-driven decision-making in cybersecurity. The ability to gather, analyse, and act on information is crucial in identifying and mitigating risks.
10. **Information Protection and Maintenance**: The need to "*Collect, evaluate, maintain and protect auditing information*" implies a growing concern for not just the acquisition of data but also its secure management and retention.

These insights reflect an expanding scope of cybersecurity roles, where technical skills are being augmented with strategic, analytical, and interpersonal competencies. It suggests a holistic approach to cybersecurity education and practice, emphasising adaptability, continuous learning, and a blend of technical and soft skills.

7.2 Analysis of the Academic & Industry Review of the ECSF Knowledge Areas:

The ECSF framework has 67 knowledge areas which are utilised across the 12 role profiles. The review identified existing knowledge areas that are recommended to be applied to other roles in the framework. Table 2 below indicates the number of knowledge areas that apply to the role profiles (ECSF Total). The total column shows the total number of knowledge areas in each role after the addition of existing ECSF knowledge areas to the roles (Total). The new column identified the total number of new knowledge areas identified and the priority columns indicates the priority assigned through the review process (Priority 5 = High, Priority 1 = Low). New knowledge areas are often ascribed a high importance, with many falling under "Priority 4" demonstrating their significance in the current landscape. Conversely, the foundational knowledge areas remain critical, with "Priority 5" being the most frequently assigned, showing the continued relevance of established knowledge in the field. This prioritisation reflects a recognition of both enduring and emerging knowledge areas within cybersecurity.

Role	Knowledge Areas by Priority							
	ECSF Total	Total	New	Priority 5	Priority 4	Priority 3	Priority 2	Priority 1
CISO	11	16	5	4	10	0	0	2
Penetration Tester	12	17	5	7	8	1	1	0
Cyber Incident Responder	15	22	7	5	11	2	0	4
Cyber Legal Policy & Compliance Officer	5	6	1	3	3	0	0	0
Cyber Threat Intelligence Specialist	13	32	19	8	3	11	2	8
Cybersecurity Architect	15	15	0	4	6	2	3	0
Cybersecurity Auditor	6	8	2	3	5	0	0	0
Cybersecurity Educator	8	14	6	1	3	2	4	4
Cybersecurity Researcher	5	8	3	3	1	1	3	0
Digital Forensics Investigator	13	22	9	3	7	1	2	9
Cybersecurity Implementor	11	18	7	7	11	0	0	0
Cybersecurity Risk Manager	10	11	1	4	3	2	0	1

Table 2: Knowledge Areas by Role and Priority

The ten new knowledge areas most frequently cited across ECSF role profiles include *an understanding of current cybersecurity trends* and *advanced persistent threats (APTs)*, both of which are critical in the current digital landscape. There is also a focus on the *multidisciplinary nature of cybersecurity, risk management strategies, and familiarity with relevant laws and regulations*. *Awareness of general cybersecurity risks, ethical considerations within cybersecurity organisations,* and *knowledge of offensive and defensive security procedures* are also key. Additionally, there's an emphasis on *legal and regulatory requirements* concerning the release and use of cybersecurity technologies, as well as *compliance obligations*.

1. **Understanding of Current Cybersecurity Trends**: Stay informed about the latest patterns and methods used in cyber threats and protective measures.
2. **Advanced Persistent Threats (APTs)**: Gain in-depth knowledge of sophisticated, prolonged cyber-attacks aimed at stealing information from organisations.
3. **Multidisciplinary Nature of Cybersecurity**: Recognise the intersection of technology, psychology, law, and management in cybersecurity practices.
4. **Risk Management Strategies**: Develop skills to identify, evaluate, and prioritise risks, and implement strategies to mitigate them.

5. **Familiarity with Relevant Laws and Regulations**: Understand the legal framework that governs data protection, privacy, and information security.
6. **Awareness of General Cybersecurity Risks**: Be aware of the common vulnerabilities and threats that affect systems and networks.
7. **Ethical Considerations within Cybersecurity Organisations**: Uphold moral principles and standards when dealing with sensitive information and cybersecurity measures.
8. **Knowledge of Offensive and Defensive Security Procedures**: Learn both how to protect against (defensive) and simulate (offensive) cyber-attacks to strengthen security.
9. **Legal and Regulatory Requirements for Release and Use of Cybersecurity Technologies**: Comprehend the legal obligations associated with the deployment and utilisation of cybersecurity solutions.
10. **Compliance Obligations**: Maintain knowledge of and adhere to regulations and standards that organisations must comply with in their cybersecurity practices.

Identifying these top 10 knowledge areas as new and necessary across the ECSF role profiles offers insights into the cybersecurity landscape and the expertise needed to navigate it. The repeated references to "*Cybersecurity trends*" in the ECSF role profiles highlight the field's evolving nature and the need for professionals to engage in continuous learning. The focus on "*advanced and persistent cyber threats*" reflects a heightened awareness of complex, ongoing cyber risks, necessitating advanced defensive strategies. The inclusion of "*multidiscipline aspect of cybersecurity*" acknowledges its intersection with various fields, while "*risk management recommendations and best practices*" emphasises a proactive stance in risk mitigation. Additionally, multiple new knowledge areas addressing laws and regulations underline the importance of legal and regulatory understanding for compliance. The recognition of "*ethical cybersecurity organisation requirements,*" alongside knowledge in both *offensive and defensive security procedures*, suggests a balanced and ethical approach is essential. Awareness of the *broader impacts of cybersecurity technology release and usage*, coupled with a strong grasp of *compliance and best practices*, reflects the industry's shift towards a more integrated and standards-driven approach.

Overall, these new knowledge areas reflect a wide range of topics underscoring a shift towards a more integrated, multidisciplinary, and proactive approach in cybersecurity. They reflect the industry's response to complex and evolving challenges, emphasising not just technical skills but also legal, ethical, and strategic thinking.

7.3 Analysis of the Online Survey:

The online survey was deployed with the aspiration of engaging respondents from various organisational backgrounds within the cybersecurity domain. While not explicitly targeted towards specific organisations, the aim was to attract participants from entities whose primary focus is cybersecurity, those with dedicated cybersecurity divisions, and those where cybersecurity plays a pivotal role in safeguarding assets and data. By casting a wide net and welcoming input from professionals across different organisational structures, the survey sought to capture diverse perspectives and insights on the roles, knowledge areas, and skills pertinent to cybersecurity across various industry contexts. This inclusive approach aimed to foster a comprehensive understanding of the cybersecurity landscape.

The online survey hosted in Survey Monkey was opened on 18th December 2023 and closed on 16th January 2024. In designing the survey each step was carefully planned and executed, starting by setting a clear objective to guide the creation of focused and relevant questions. The survey was structured logically, with questions phrased using plain English principles, encompassing a variety of formats including multiple-choice and open-ended responses. The survey was designed to be concise (the average was 11 minutes to complete), in anticipation of a higher completion rate, and was optimised for mobile devices to facilitate accessibility. Prior to the survey's launch, a pilot test was conducted to address any potential issues. The utmost importance was placed on maintaining respondents' privacy and anonymity. Clear instructions and an explanatory introduction were provided at the outset. Effective distribution strategies were employed, and a detailed plan for data analysis was defined.

The total number of responses to the survey was 206. Responses from countries outside the EU were removed resulting in 190 valid responses.

Country	Percent	Responses
Ireland	30%	57
Romania	27%	51
Croatia	12%	23
Italy	9%	17
Belgium	5%	9
Lithuania	5%	9
Germany	3%	5
Estonia	2%	4
Poland	2%	4
Czech Republic	2%	3
Slovakia	1%	2
Spain	1%	2
Sweden	1%	2
Cyprus	1%	1
Greece	1%	1

Table 3: Survey Responses by Country

The countries with the largest number of respondents are Ireland (57) representing 30% of respondents, Romania with (51) respondents or 27%, Croatia with (23) responses or 12% and Italy (17) responses or 9%. The remaining 11 countries had responses between 9 and 1 and accounted for 22% of the overall responses as seen in table 3 above. The survey results are heavily weighted towards Irish and Romanian perspectives, which may not accurately represent the broader European context. This could lead to biased conclusions if the data is generalised across Europe. Conclusions drawn from this data should be taken with care, acknowledging the overrepresentation of certain countries and underrepresentation of others.

Organisation Types

The survey data presents a breakdown of the types of organisations respondents are affiliated with. The majority work for Small Medium Enterprises (SMEs), accounting for 34% or 65 respondents. Multinational Corporations (MNCs) follow with 28%, representing 53 individual respondents. Governmental Organisations or Departments are the employers of 15% or 28 of the participants. Private Training Providers make up 7% (14 respondents) and the 'Other' category, which includes organisations identified as “private companies, industry associations, clusters and limited companies”, account for 6% (12 respondents). Academic Institutions constitute 6%, which translates to 11 respondents, and the fewest work for Non-governmental

Organisations (NGOs), at 4% or 7 individuals. This distribution highlighted in chart 1 below, provides insight into the diverse organisational backgrounds of the survey participants.

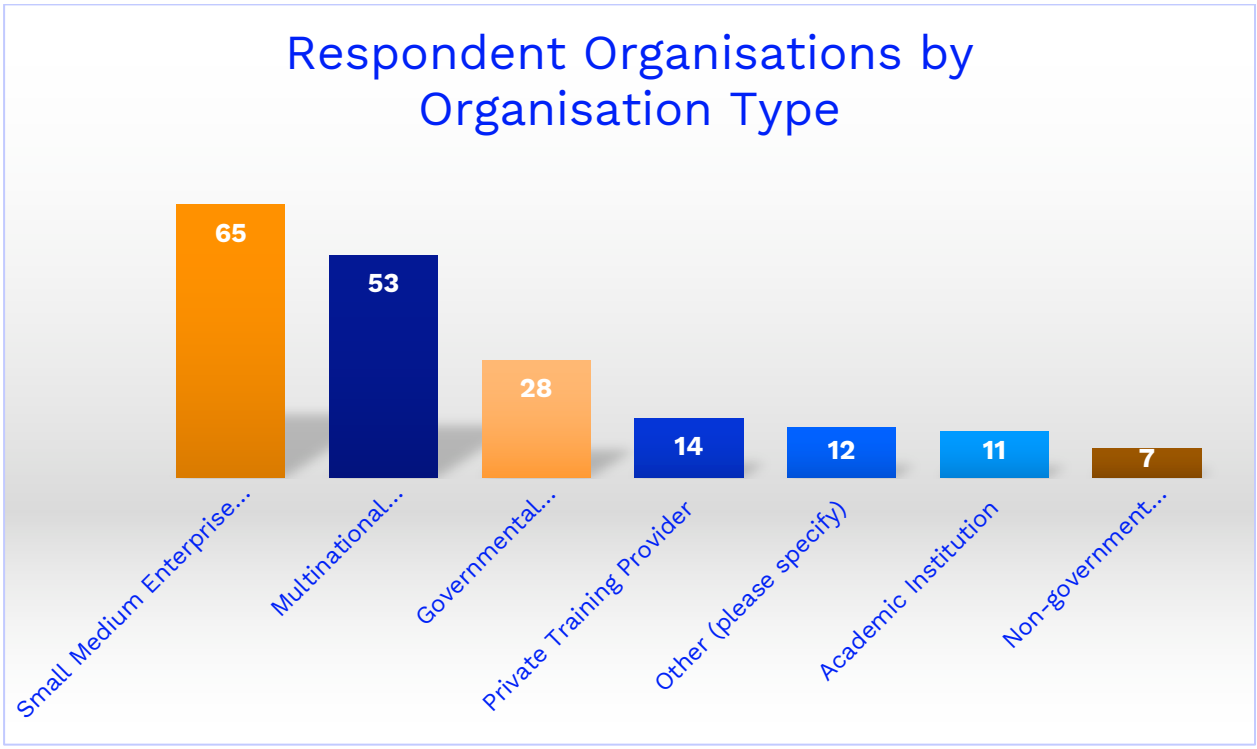

Chart 1: Type of Organisations where the Survey Respondents Work

The survey data reflects the professional diversity of the respondents within the realm of cybersecurity and related fields. A significant portion, 31%, hold leadership roles in cybersecurity, while ICT professionals make up 20%. Business management roles account for 17%, followed by cybersecurity practitioners at 12%. Respondents who chose 'Other' (10%) identified themselves in specialised roles such as IT managers, cybersecurity researchers, auditors, consultants, and educators, indicating the survey reached a wide spectrum of professionals engaged in various capacities related to cybersecurity.

In the surveyed group, the majority, 43% or 82 respondents, view cybersecurity as an essential activity for the protection of their organisation or business. Nearly a third, at 29% or 56

respondents, are from companies for whom cybersecurity is the core business. Meanwhile, 27% or 52 respondents work for companies that have a dedicated cybersecurity division or business, indicating that cybersecurity is a significant, but not the sole, focus of their operations. This data illustrates the varying degrees to which the surveyed organisations are involved in cybersecurity.

Smart Technologies & Sensitive Data

The survey indicates that 41% of organisations are active in the smart tech industry. Moreover, a notable 78% handle sensitive data that would potentially appeal to cyber criminals, emphasising the vital role of cybersecurity. Only 22% reported not managing sensitive data, which underscores the heightened need for robust cybersecurity practices in most organisations, especially those dealing with sensitive data.

Those respondents who are involved in smart technologies and, or handle sensitive data identified the following skills they require to ensure they keep their technologies and data safe. Table 4 summarises the primary skills as identified by the respondents.

Skills Required to Protect Smart Technologies and Data	Responses
Network & Operating Systems	22
Risk Management	17
Cloud & Web (12 & 3 respectively)	15
Incident Response	12
Data Privacy	10
Individual Awareness (Stakeholders, Managers, Employees, HR)	9
Artificial Intelligence (AI)	9
Cryptography	8
Encryption	8
Regulations	8
Audit	4
Digital Forensics	4
GDPR, Dora, NIST	4

Table 4: Skills Required to Protect Smart Technologies & Sensitive Data

The respondents' feedback on the skills needed to protect smart technologies and sensitive data provides several insights. Technical proficiency, particularly in "*Network & Operating Systems*," is paramount, reflecting the necessity of managing the infrastructure critical to

smart technologies. "*Risk Management*" and "*Incident Response*" skills are crucial for pre-empting and addressing cybersecurity incidents. The importance of "*Cloud & Web*" skills corresponds with the increasing reliance on cloud services, while "*Data Privacy*" and understanding "*Regulations*" like GDPR highlight the need for compliance and personal data protection. *"Individual Awareness*" emphasises the human aspect of cybersecurity, "*Artificial Intelligence (AI)*" underscores its growing significance as a technology in its own right and also in the field of cybersecurity. The need for "*Cryptography*" and "*Digital Forensics*" skills illustrates the importance of securing data and conducting in-depth threat analysis.

This spread of skills indicates a comprehensive approach to cybersecurity education and practice, recognising the importance of a broad skill set that includes both technical expertise and a strategic understanding of risk management, regulatory environments, and the human elements of cybersecurity.

Cybersecurity Roles

Respondents were asked to identify the first and second most needed cybersecurity roles in their organisation which are illustrated in chart 2 below. The role of Chief Information Security Officer (CISO) emerges as the most needed role with the highest percentage of responses (23%). Cybersecurity Threat Intelligence Specialists and Cybersecurity Educators are also highly valued, each receiving 17% of responses, which illustrates a balanced need for roles focusing on proactive threat management and educational capabilities in cybersecurity within industry. When considering the second most needed role, Cybersecurity Threat Intelligence Specialists again rank highly, this time with a slightly increased percentage (21%), suggesting their pivotal role in ongoing security operations and strategy.

Cybersecurity Risk Managers and Cybersecurity Legal, Policy & Compliance Officers are closely behind in importance, with 20% and 19.5% of responses, respectively, highlighting the emphasis on managing cybersecurity risks and ensuring compliance with legal and policy frameworks as critical functions in organisations.

Chart 2: Most Needed Cybersecurity Roles in the Respondents Organisations

Skills for Cybersecurity Professionals

The respondents were asked to identify the three most important skills for cybersecurity professionals. The responses were aggregated and analysed to identify the prevalent trends and patterns. The analysis of responses yielded a comprehensive list of 17 professional skills. The frequency of selection for each skill varied, providing insights into the relative importance attributed by the respondents. Artificial Intelligence (AI) was selected 64 times, indicating a widespread recognition of the importance of AI in enhancing cybersecurity measures through advanced threat detection and response mechanisms. Law/Legal, Policy & Ethics was chosen 54 times followed by Risk which was selected 46 times. Business acumen and incident management are also rank highly emphasising the need for professionals who understand business processes and can effectively respond to security incidents.

Additionally the respondents identified a range of transversal skills deemed essential for cybersecurity professionals. These skills, while not specific to the technical aspects of cybersecurity, play a pivotal role in shaping an individual's effectiveness in this domain. The top transversal skills, along with their frequencies include Communications selected 39 times, highlighting the importance of clear and concrete communication skills in facilitating

collaboration and knowledge sharing. The second highest transversal skill is leadership/management selected 11 times followed by project management selected 5 times underscores the importance of effective communication and leadership in managing cybersecurity initiatives. Other soft skills such as Analytical Skills, Change Management and Adaptability are recognised but to a lesser extent, suggesting a balanced approach where technical expertise and soft skills complement each other in cybersecurity roles. Table 5 below reflects the professional and transversal skills identified.

Professional Skills	Score	Transversal Skills	Score
AI	64	Communications	39
Law/Legal, Policy, Ethics	54	Leadership/Management Skills	11
Risk	46	Project Management	5
Threat Management/Analysis	43	Stakeholder Management	2
Business / Business Process	42	Analytical Skills	2
Incident Management	22	Change Management	2
Intelligence Analysis	20	Adaptability	2
Cloud	13	Problem Solving	2
Compliance	10	Decision Making	1
Forensics	9	Critical Thinking	1
Governance	7	Report Writing	1
Privacy / Data Privacy	6	Mentoring/Tutoring	1
Testing	6	Methodical Working	1
Audit	4		
Blockchain	3		
Automation	3		
Geopolitical	2		

Table 5: Most In Demand Professional and Transversal Skills

Knowledge Areas and Skills for Cybersecurity Management Roles

The survey respondents were asked to identify the three most important knowledge areas and skills needed for cybersecurity management roles. The responses suggested a strong emphasis on Risk & Governance, with over half of the respondents (53%) identifying it as crucial. This indicates a recognition of the need for robust governance structures and risk assessment capabilities in managing cybersecurity effectively. Additionally, nearly half of the respondents highlighted the importance of Management Skills for Cybersecurity (47%) and Cybersecurity Strategy & Alignment to the Business Strategy (43%), reflecting an understanding that effective cybersecurity is not just about technical knowledge but also about strategic integration within the business coupled with strong leadership abilities. While other areas such as Data Security Management and Cybersecurity Standards/Certifications

are noted, they are seen as less critical compared to overarching strategy and management skills. This data as outlined in table 6 below points to a trend where soft skills and business acumen are increasingly valued alongside traditional cybersecurity competencies.

Knowledge Areas and Skills Required for Cybersecurity Management Roles	Percent	Responses
Risk and Governance	53%	101
Management Skills for Cybersecurity	47%	90
Cybersecurity Strategy & Alignment to the Business Strategy	43%	82
Understanding Cyber Threats	24%	45
Business Continuity Management	24%	45
Data Security Management	21%	40
Cybersecurity Standards / Certifications	20%	38
Data Value & Risk Management	16%	31
Organisational Risk Reviews	14%	26
Audits and Testing	9%	18
Cybersecurity Ethical Standards	9%	18
Collaborative Cybersecurity	8%	15
Cyber Intelligence	6%	11
Collective Cybersecurity	5%	10

Table 6: Knowledge Areas & Skills required for Cybersecurity Management Roles

Knowledge Areas and Skills for Cybersecurity Technology Roles

The responses to the question which sought to identify the most important knowledge areas and skills for cybersecurity technology roles, reveals a strong consensus on the foundational aspects of cybersecurity as seen in table 7 below. Cybersecurity Architecture (59%), Systems Security (58%), and Network Security (57%) are the top three areas identified, emphasising the critical importance of securing the underlying frameworks and networks that support technology infrastructure. While there is significant interest in the Cybersecurity of AI (29%) and emerging technologies like Blockchain and Quantum (26%), these areas are considered less immediate compared to the core security domains. Security in the context of remote work and securing devices also registers notable concern (28%), likely reflecting the shift towards remote and hybrid work models and the consequent security challenges. Other areas such as IoT Security, Data Analytics in Cybersecurity, and Privacy Enhancing Technologies receive less emphasis, indicating that while these areas are relevant, they may be seen as specialised or secondary in the broader landscape of cybersecurity technology roles.

Knowledge Areas and Skills required for Technology Roles	Percent	Responses
Cybersecurity Architecture	59%	113
Systems Security	58%	110
Network Security	57%	108
Cybersecurity of AI	29%	56
Remote work and collaborative environments protection & securing shared/private devices	28%	53
Cybersecurity and Emerging Technologies such as Crypto, Blockchain, Quantum, Robotics, Open Source	26%	49
Data Analytics in Cybersecurity	18%	34
IoT Security	12%	23
Privacy enhancing technologies	7%	14
Cybersecurity of open social media platforms	5%	10

Table 7: Knowledge Areas & Skills required for Technical Cybersecurity Roles

Knowledge Areas and Skills for Regulatory Roles

Respondents identified the three most important knowledge areas and skills for regulatory roles, as Cybersecurity Related Regulations at (59%). This is closely followed by European Policies and Privacy Issues such as GDPR, each at 53%, indicating a strong focus on compliance with European legislative frameworks and data protection standards. There is also a significant emphasis on understanding specific legislation such as the Cyber Act and AI Act, as well as Legal & Ethical Frameworks, both at 38%, reflecting the complex legal landscape that professionals in regulatory roles must navigate. Less prioritised, but still recognised are the broader Cybersecurity Ecosystem and the need for Trans-institutional, Cross Border Cooperation and Regulatory Frameworks. Cyber Diplomacy is the least prioritised area, suggesting it may be an emerging concern within the regulatory space as outlined in table 8 below. Overall, the responses underscore a need for regulatory professionals to be well-versed in a mixture of specific laws, ethical considerations, and overarching policy frameworks.

Knowledge Areas and Skills required for Regulatory Roles	Percent	Responses
Cybersecurity Related Regulations	59%	113
European Policies	53%	100
Privacy Issues (GDPR etc.)	53%	100
Cyber Act & AI Act	38%	73
Legal & Ethical Frameworks	38%	73
Cybersecurity Ecosystem	25%	48
Trans-institutional, Cross Border Cooperation and Regulatory Frameworks	23%	44
Cyber Diplomacy	10%	19

Table 8: Knowledge Areas & Skills Required for Regulatory Roles

Knowledge Areas and Skills for Cybersecurity Response Roles

In identifying the three most important knowledge and skills for Cybersecurity Response Roles, the critical competency, is identified as *Incident & Crisis Management* by 87% of respondents. This suggests a strong consensus on the need for immediate and effective action when security breaches occur. Additionally, the significant importance placed on *Computer Network Forensics and Malware Analysis* (42%) and *Strategic & Crisis Communications* (44%) reflects the necessity for technical investigative capabilities alongside clear and decisive communication in times of crisis. Other areas such as *Managing Cyber Response Teams, Network Visualisation and Vulnerability Detection* are recognised as important, but to a lesser extent, indicating that while *team leadership* and *technical assessment* skills are valuable, the priority is on direct crisis resolution and *communication* skills as outlined in table 9 below. This data underlines the complex nature of cybersecurity response roles, requiring a blend of strategic, technical, and communication skills.

Knowledge Areas and Skills required for Cybersecurity Response Roles	Percent	Responses
Incident & Crisis Management	87%	166
Strategic & Crisis Communications	44%	83
Computer Network Forensics and Malware Analysis	42%	79
Managing Cyber Response Teams	39%	75
Network Visualisation and Vulnerability Detection	26%	50
Organisational Cyber Education	24%	46
Collaboration with Law Enforcement and the Judicial System	23%	44
Cybersecurity Cultural Engineering	14%	27

Table 9: Knowledge Areas & Skills required for Cybersecurity Response Roles

Transversal Skills for Cybersecurity Management Roles

Respondents identified the three transversal skills deemed essential for cybersecurity management roles. *Communication & Collaboration* top the list with 87% of respondents identifying these as crucial, highlighting the importance of effective interpersonal skills in the management of cybersecurity. *Strategic Thinking & Decision Making* follows with 73%, indicating that the ability to analyse situations and make informed decisions is highly valued. Other skills like *Strategic Relationship Management, Education & Training Delivery*, and *Workforce Leadership* are also recognised but to a lesser extent, suggesting that while these skills are important, they are secondary to the core capabilities of *communication and strategic decision-making*. *IT Project Management* is considered important by 25% of the respondents, reflecting its role in the implementation of cybersecurity projects. Overall, these responses underscore the multifaceted nature of cybersecurity management, requiring a combination of interpersonal, strategy, and leadership skills as outlined in table 10 below.

Transversal Skills Required for Cybersecurity Management Roles	Percent	Responses
Communication & Collaboration	87%	165
Strategic Thinking & Decision Making	73%	139
Strategic Relationship Management	42%	79
Education & Training Delivery	39%	75
Workforce Leadership	34%	64
IT Project Management	25%	48

Table 10: Transversal Skills required for Cybersecurity Management Roles

Technical Skills for Cybersecurity Management Roles

The responses to the question seeking to identify the three technical skills needed for Cybersecurity Management roles underscore the significance of technical acumen in cybersecurity management roles, with *Technology Fluency* being identified as the most critical skill by 73% of respondents. This is closely followed by *Enterprise Architecture and Infrastructure Design* at 69%, highlighting the necessity to understand the design of robust cybersecurity frameworks. *Network Fundamentals* also emerge as a key skill area with 55% of the responses, reflecting the foundational role of networking in cybersecurity. *System Administration Knowledge* and *Cloud Computing* are acknowledged by over 40% of participants, indicating the growing relevance of cloud services and system management in cybersecurity strategies. *Database Management Fundamentals*, while still important, is considered less critical, with 20% of respondents noting it as a required skill. These insights

reveal a clear demand for comprehensive technical skills that encompass a range of areas from basic network security to more advanced technology systems and cloud-based infrastructure in the field of cybersecurity management as outlined in table 11 below.

Technical Skills Required for Cybersecurity Management Roles	Percent	Responses
Technology Fluency	73%	139
Enterprise Architecture and Infrastructure Design	69%	132
Network Fundamentals	55%	104
System Administration Knowledge	42%	79
Cloud Computing	41%	78
Database Management Fundamentals	20%	38

Table 11: Technical Skills required for Cybersecurity Management Roles

Programme Delivery Models

The most popular delivery model for the DIGITAL4Business Master's identified by 36% (68) respondents, is the blended learning model that combines online resources and offline events, indicating that a mix of digital convenience and in-person engagement is attractive to a significant portion of respondents. Following this, 24% (45) respondents show a preference for modules that offer micro-credentials, suggesting a notable interest in flexible learning options that provide tangible acknowledgments of specific skill sets. Close behind, with 23% (43) respondents, is the preference for an online programme supplemented by physical events, which implies that learners still value face-to-face interactions and networking opportunities. Lastly, the fully online programme delivered on a digital platform received the least interest, with 18% (34) respondents selecting this option, indicating that while there is a demand for completely online learning, it may be less appealing than models which incorporate some level of offline engagement. Overall, these insights should guide the academic partners in designing the Cybersecurity Masters programmes to meet the diverse learning preferences of their prospective students.

The survey responses indicate a clear preference for the duration of the DIGITAL4Security Master's Programme among potential candidates. A majority, 56% (106) of respondents, favour a 2-year part-time programme. This suggests that many individuals are likely seeking to balance their education with other commitments, such as work or personal responsibilities, and thus prefer a programme that is spread out over a longer period to allow for flexibility. In contrast, 27% (52) of respondents are inclined towards a more intensive 1-year full-time

programme, indicating a desire for a quicker completion and possibly a faster transition to advanced career opportunities. The least preferred option, with 17% (32) of responses, is a 2-year full-time programme, which might suggest that a significant time commitment without the flexibility of part-time study is less appealing for those considering a Cybersecurity Master's Programme. These insights should inform the consortium when considering programme structures that align with the needs and lifestyles of their target student demographic.

7.4 Analysis following the Review of Cybersecurity Reports and Publications

In synthesising the findings from the DIGITAL4Security needs analysis with other published reports and surveys, the overarching narrative is clear: *both soft and hard skills are integral to cybersecurity roles*.

The DIGITAL4Security needs analysis prioritises communication, collaboration, and strategic thinking confirmed through the survey by 87% of respondents as key in their roles, which aligns with Cyber Ireland's, (2023) "State of the Cyber Security Labour Market in Ireland" report which also underscores these soft skills alongside technical and risk management skills. Central to this is the art of *communication*, where professionals are expected to effectively engage with stakeholders. The nature of cybersecurity demands a *collaborative approach*, making teamwork a key focus. *Technical acumen*, especially in integrating and assessing cybersecurity measures within organisational frameworks, is also stressed, along with proficiency in *navigating the technical landscape*. Additionally, expertise in *risk management* and *governance* is underscored as vital. *Creativity* and *analytical prowess* are considered essential to adapt to the dynamic cybersecurity environment. Lastly, the Cyber Ireland report notes an increased need for specialisation across roles, illustrating a trend towards more distinct and interconnected positions, mirroring observations from the DIGITAL4Security needs analysis. This is further emphasised by CISCO (2022) in their report which calls out the importance of *technical proficiency* combined with a strong understanding of *risk management*, *teamwork,* and strategic planning which CISCO see as crucial in the face of evolving cyber threats and complex technology landscapes.

The Global Cybersecurity Outlook (WEF, 2022) highlights the need for leaders to be knowledgeable about *emerging technologies* and *cyber resilience*, spotlighting the challenges posed by technological advancements such as generative AI and the corresponding skills gap.

It provides crucial insights into the multifaceted challenges facing leaders in the area of cybersecurity. Technological advancements including the rise of AI brings new challenges and opportunities for cybersecurity leaders. There is an increasing gap in organisational cybersecurity capabilities reinforcing the need for cybersecurity leaders to build resilience and enable their organisations to address potential cybersecurity threats. Leaders face challenges in building cyber-resilience in their organisations due to skills shortages. Some of these key takeaways align with the insights obtained from the DIGITAL4Security needs analysis. Overall the report is a call to action for leaders to address these issues and build robust cybersecurity into their organisations by staying informed about the trends and understanding their implications so that their organisation can successfully navigate the ever evolving cybersecurity landscape.

This sentiment is echoed by Dal Cin et al., (2023) who advance this discussion by identifying 'cyber transformers' who integrate cybersecurity into their business strategies, indicating a trend towards a business-led cybersecurity approach. They emphasise that organisations with a holistic understanding of cybersecurity risk, and those leveraging AI demonstrate a more advanced cybersecurity posture. They also advocate the need for clear communication strategies and collaboration with government agencies to address external cyber threats and breaches effectively. Additionally, this study outlines the attributes and practices that differentiate "cyber transformers" from other organisations, acknowledging the attributes of the business-led CISO and the integration of cybersecurity risk into the organisation's risk management practices and the necessity of aligning cybersecurity with evolving business needs

Aligning the cybersecurity strategy with the business strategy ensures that security measures directly support the organisation's objectives and core functions, thereby enhancing resilience and competitive advantage in a landscape where cyber threats can significantly impact

business continuity and reputation. Aligning with the DIGITAL4Security needs analysis, this report identifies the need for cybersecurity professionals to not only have technical expertise but to possess transversal skills and also understand the broader business goals and challenges. This convergence demands a skill set that includes *strategic planning*, *risk assessment*, and the ability to *communicate complex security concepts* in the context of business outcomes, ensuring security initiatives enhance business value and resilience.

Rodgers, McCurdy and Parham, (2023) in a joint report published by IBM and AWS advise organisations to integrate their data, operations, technology, and security with their core business goals, to enhance security and trust, which in turn drives better decision-making and performance. The report highlights the value for organisations in *aligning their security strategies to the organisation's primary business objective*, or "North Star," to help strengthen data security and establish the trust required to fuel better decisions and better performance. The report emphasises the importance of a *collaborative culture* in connecting various functional strategies to spur *innovation*. It also points out that organisations leading in data management prioritise cybersecurity and data ethics. They place a stronger emphasis than peers on cybersecurity and data ethics, on transparency in data architecture, and on trust in data effectiveness. Leaders who create an environment where collaboration is the norm and where functional strategies are connected, power innovation at scale and speed.

The authors also call out a recent Salesforce survey which notes that the most senior IT leaders expect generative AI to help their organisations take better advantage of data to serve customers and operate more efficiently. But 71% expect it to introduce new security risks to their data. The report suggests that leveraging generative AI for cybersecurity requires robust AI ethics and governance to balance the potential risks and rewards. When engaging in generative AI projects, business leaders must ensure they establish strong *AI ethics* and *governance* mechanisms to mitigate the risks involved. To facilitate the responsible use of generative AI, leaders need to implement security policies and controls that recognise both offensive and defensive use cases. Generative AI offers defensive advantages and can simulate cyber-attacks that strengthen an organisation's training and readiness. Leaders must encourage a culture that values secure and trusted data, promote data security practices at all organisational levels, and redefine them as key to performance enhancement. Broadening

the diversity of skills and perspectives in security teams, and incorporating security and privacy responsibilities into all job roles, increases business value through robust data privacy and ethics practices.

Cyber Ireland's (2023) State of the Cyber Security Labour Market report also identified the most in-demand cybersecurity roles and skills. A comparison between the Cyber Labour Market Report and the DIGITAL4Security needs analysis reveals several congruent and complementary findings concerning the demand for specific cybersecurity skills and roles. Both underscore the critical importance of *technical skills* within the field. The Cyber Labour Market Report delineates essential competencies for Cyber Security Implementers, such as *solution integration* and *security assessment*, which aligns with the DIGITAL4Security's identification of *Systems Security* and *Network Security* as key technical areas.

Furthermore, the role of Cyber Incident Responders, highlighted in the Cyber Labour Market Report, necessitates proficiency in *incident handling, threat analysis*, and *system operation*. This requirement resonates with the emphasis placed by the DIGITAL4Security needs analysis on the significance of *Incident Response* and the *management of cybersecurity incidents and threats*. In the realm of risk management, skills in *risk analysis* and *compliance* are identified as crucial for Cyber Security Risk Managers, paralleling DIGITAL4Security's focus on Risk Management as a vital skill area.

Additionally, both acknowledge the necessity of *communication and collaboration* skills across various cybersecurity roles. Both also converge on the need for *strategic thinking, decision-making*, and other transversal skills, suggesting a trend towards a more integrative and holistic approach in cybersecurity roles.

Regarding in-demand roles, the DIGITAL4Security needs analysis identifies positions such as the Chief Information Security Officer (CISO), Cybersecurity Threat Intelligence Specialists, and Cybersecurity Educators as particularly sought after, aligning with the range of specialised cybersecurity roles highlighted in the Cyber Labour Market Report.

In summary, both the DIGITAL4Security Needs Analysis and the Cyber Labour Market Report collectively illustrate a consistent and evolving landscape of requirements in the cybersecurity field, indicating a growing need for a combination of technical, strategic, analytical, and interpersonal competencies.

Collectively, these studies and reports align with the DIGITAL4Security needs analysis and underscore a multifaceted cybersecurity landscape demanding a blend of interpersonal, strategy, technical, and business-aligned skills. In essence, they paint a picture of a dynamic field that values a blend of strategic, technical, and soft skills to combat evolving cyber threats. The commonalities suggest that while the cybersecurity field is diverse and evolving, there is a core set of skills that are widely recognised as essential across a variety of roles. These include not only technical abilities but also soft skills such as communication and collaboration, as well as an understanding of risk management and governance.

7.5 Analysis following the Review of Cybersecurity Research

A number of cybersecurity related research projects focusing on cybersecurity skills needs were reviewed and the following summarises the main findings.

The REWIRE Project (2022) based their cybersecurity skills research creating the REWIRE framework based on the ENISA and mapped between NICE NIST competencies and the ENISA framework creating a mapping to existing courses and schemes. The project organised competencies into three distinct categories for the REWIRE project: Cybersecurity Skills, IT Skills, and Soft Skills.

The competencies categorised under Cybersecurity Skills encompass the essential tasks, knowledge and skills necessary for roles within cybersecurity, while IT Skills refer to foundational knowledge in information technology that does not directly involve security aspects. Lastly, Soft Skills encompass the non-technical knowledge, skills, and abilities vital for professional success.

The REWIRE and DIGITAL4Security needs analysis, both focus on cybersecurity skills and roles, and exhibit notable parallels in their findings. Each underscores the criticality of technical skills, particularly in areas like Information Systems and Network Security, as well as Operating Systems and Threat Analysis. Furthermore, they both highlight the essential role of soft skills, especially in communication and collaboration, for effective cybersecurity management. Risk management and security assessment capabilities are also identified as key competencies. Additionally, both pinpoint a high demand for specific roles such as Chief Information Security Officers and Cybersecurity Educators, indicating a need for leadership and educational expertise in the field. The importance of innovation and creativity in addressing cybersecurity challenges is acknowledged, reflecting the dynamic and adaptive nature of the field. Lastly, both emphasise the growing significance of legal and ethical considerations in cybersecurity, underlining the need for compliance and ethical integrity. These findings suggest a holistic approach to cybersecurity education and practice, integrating a blend of technical, strategic, and interpersonal skills.

The CyberSecPro project, emphasises the need for practical and hands-on training, industry-academia collaboration, and a focus on upskilling and reskilling. Both the CyberSecPro project and DIGITAL4Security needs analysis converge on critical aspects of cybersecurity skills and roles, underscoring a multifaceted approach as imperative in this domain. Both accentuate the escalating importance of proficient interpersonal skills, including clear communication with a diverse array of stakeholders, effective teamwork, and adept coordination, establishing these as fundamental in the realm of cybersecurity. Furthermore, they assert the necessity for technical expertise, which encompasses a comprehensive understanding of contemporary cybersecurity trends, the landscape of advanced threats, and proficient risk management strategies. Both also underline the significance of skills pertinent to the integration of cybersecurity solutions, remaining current with technological advancements, and the foresight to anticipate imminent threats.

Given the intricate and varied nature of challenges in cybersecurity, both CyberSecPro and DIGITAL4Security' needs analysis advocate for the adoption of creative and innovative problem-solving methodologies. A consensus is evident in their emphasis on the pivotal role of proactive threat management and the requirement for meticulous assessments of both the security and performance of various technological solutions in the organisation. Additionally,

they underscore the criticality of ethical considerations, legal acumen, and the upholding of integrity within cybersecurity practices. Moreover, the DIGITAL4Security needs analysis draws attention to the paramount importance of strategic thinking, informed decision-making, and other cross-functional skills in cybersecurity management roles. Abilities in strategic relationship management, the delivery of education and training, and leadership in workforce management are recognised as critical, aligning with the holistic approach also championed in the CyberSecPro skills gap report.

These overlapping insights from both projects illustrate a consistent understanding of the evolving requirements in the cybersecurity field, pointing towards an integrative blend of technical, strategic, analytical, and interpersonal competencies that are increasingly sought after.

8. FINDINGS AND RECOMMENDATIONS

8.1 Insights and Implications (Roles)

The DIGITAL4Security needs analysis set out to focus on addressing knowledge and skills needs for the 7 roles of; Chief Information Security Officer (CISO), Cyber Threat Intelligence Specialist, Cybersecurity Educator, Digital Forensics Investigator, Cybersecurity Auditor, Cybersecurity Risk Manager and Cyber Legal, Policy, & Compliance Officer. Comparatively, the Digital Forensics Investigator role is distinctly focused on the technical and ethical aspects of collecting and analysing digital evidence, which is less emphasised in the other roles. For instance, roles such as Cyber Legal Policy & Compliance Officer and Cybersecurity Auditor, have a stronger focus on compliance, legal aspects, and auditing, respectively. The Cyber Threat Intelligence Specialist and Cybersecurity Educator roles are more oriented towards analysis, training, and education in cybersecurity, while the Cybersecurity Risk Manager is focused on risk management and mitigation. After careful consideration and analysis of these roles we have decided to exclude the Digital Forensics Investigator role from our master's programme curriculum. This decision stems from the recognition that the Digital Forensics Investigator role encompasses a unique set of skills and knowledge that are distinctively more technical and specialised compared to the 6 other roles. These specialised skills, particularly

those pertaining to the collection, analysis, and presentation of digital evidence, require a depth of learning and practical application that is not as central to the broader objectives of our master's programme. By focusing on areas more aligned with the leadership and strategic aspects of cybersecurity, we aim to provide well-rounded education that is relevant across the cybersecurity roles, without delving into the highly specialised domain of digital forensics.

8.2 Insights and Implications (Knowledge Areas):

1. The presence of a significant number of new knowledge areas with high priorities suggests the cybersecurity field is rapidly evolving, with emerging areas gaining importance.
2. The balance between new and original knowledge areas with various priority levels indicates the need for continuous learning and adaptation in cybersecurity roles.
3. For training and education in cybersecurity, this data underscores the importance of updating curricula to include both established and emerging knowledge areas, particularly those with higher priorities.
4. Cybersecurity professionals should focus on acquiring a broad range of knowledge, including new areas that are gaining prominence in the field.

8.3 Insights and Implications (Skills):

1. The significant presence of both new and original skills indicates a balanced focus in the cybersecurity field, valuing both foundational knowledge and emerging competencies.
2. Educational institutions and training programmes should aim to provide a comprehensive curriculum that covers both these established and emerging skills.
3. Cybersecurity professionals should maintain a focus on foundational skills while also staying abreast of new developments in the field, as indicated by the distribution of new skills across various priority levels.

Comparing and analysing the original ENISA knowledge areas and skills with the revised knowledge areas and skills provides a comprehensive view of the knowledge and skills landscape in cybersecurity, highlighting the dynamic nature of the field and the importance of the following:

The analysis reveals a broadening and specialisation in cybersecurity competencies, with the updated ENISA framework showing greater diversity and definition in skills and knowledge areas. This reflects in the detailed categorisation and identification of both transversal and professional skills. Roles within cybersecurity are evolving to be more multidisciplinary, with a stronger emphasis on integration across various domains. The refined descriptions indicate a move towards role-specific skill sets, highlighting the dynamic nature of the field and the emergence of new, role-tailored capabilities. Newly introduced colour-coded categories point to an expanded and nuanced skill set, aligning the ECSF profiles with current industry demands, ensuring they remain pertinent and responsive to the changing landscape.

Overall, the comparison shows a progression towards a more detailed, role-specific, and updated representation of necessary skills and knowledge in the field of cybersecurity, reflecting the insights gained from academic and industry evaluations.

8.4 Recommendations for the Development & Delivery of the Curriculum Framework

Based on the analysis of the data related to the ENISA ECSF knowledge areas and skills for the following roles: CISO, Cyber Legal and Compliance Officer, Threat Intelligence Specialist, Cybersecurity Auditor, Cybersecurity Educator, and Cybersecurity Risk Manager, academic institutions should consider the following when designing the master's programme:

The curriculum integration should encompass key knowledge areas and skills that are most valued in the field, including cybersecurity industry certifications, standards, methodologies, frameworks, and risk management practices. It is vital to cover a diverse range of topics that span technical, legal, regulatory, and ethical knowledge, ensuring that learners are well-versed in laws, regulations, and ethical requirements of cybersecurity. Practical skills in interpreting

data acquired from monitoring processes, test results and incident handling are necessary. In addition the ability to effectively manage stakeholders and resources should be a focus, along with tailored training for specific roles such as Cyber Legal and Compliance Officers. For educators, pedagogical skills and programme development are essential, while Cybersecurity Risk Managers need a strong foundation in risk management. Aligning with industry-recognised certifications and standards is important. The programme must also develop essential soft skills like communication, teamwork, and leadership.

By focusing on these areas, academia can create a comprehensive and dynamic master's programme that effectively addresses the learning needs of these crucial ECSF roles in cybersecurity. A blended learning model combining online resources and offline events is the favoured mechanism for the master's programme delivered on a part-time basis over a two year duration. Micro-credentials and face to face interactions are also valued, indicating the need for flexibility and networking opportunities to be included in the design of the programme. These insights underscore the importance of catering to a diverse learning preferences and balancing convenience while optimising student engagement in the curriculum.

9. REFERENCES

Cisco (2022) *Security Outcomes Report, Volume 3*, *Cisco*. Available at: https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html (Accessed: 25 January 2024).

CyberSecPro (2023) *CyberSecPro*. Available at: https://www.cybersecpro-project.eu/ (Accessed: 6 February 2024).

Dal Cin, P. *et al.* (2023) *State of Cybersecurity Resilience 2023*, *Accenture.com*. Accenture. Available at: https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf (Accessed: 25 January 2024).

European Cybersecurity Skills Framework (ECSF) (2022) *ENISA*. Available at: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework (Accessed: 26 January 2024).

Fortinet (2023) *2023 Cybersecurity Skills Gap Global Research Report*. Available at: https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf (Accessed: 24 January 2024).

REWIRE -Cybersecurity Skills Alliance A New Vision for Europe R3.3.1. Cybersecurity Skills Framework (2022). Available at: https://rewireproject.eu/wp-content/uploads/2022/11/R3.3.1.Cybersecurity-Skills-Framework_FINAL.pdf (Accessed: 6 February 2024).

Rodgers, C., McCurdy, C. and Parham, G. (2023) *Data security as business accelerator?*, *IBM*. Available at: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/data-security (Accessed: 26 January 2024).

Cyber Ireland (2023) *State of the Cyber Security Labour Market in Ireland*. Available at: https://cyberireland.ie/wp-content/uploads/2023/09/Cyber-Labour-Market-Report-2023.pdf (Accessed: 25 January 2024).

WEF (2022) *World Economic Forum - Home*, *www3.weforum.org*. Available at: https://www3.weforum.org/maintenance/public.htm (Accessed: 25 January 2024).

Work Package 2/Name	WP2 Needs Analysis and Programme Design
Deliverable Name	D2.1 Needs Analysis Report
Partners involvement	DTSL
Submission Deadline (As per Annual Work Plan)	31-02-2023

Rate	1	2	3	4	5
Quality Parameter	very low/strongly disagree	low/dis agree	moderate/ neither nor	high/ agree	very high/strongly agree
1. The work performed corresponds to the requirements and methodological standards of the project.	☐	☐	☐	☐	☐
Insert text here…Insert text here…					
2. The drafting and structuring of each deliverable include the contribution of all relevant experts.	☐	☐	☐	☐	☐
Insert text here…Insert text here…					
3. Deliverables use clear and easily understandable language in the text and the design is professional and in line with the project brand identity, guidelines, and document template.	☐	☐	☐	☐	☐
Insert text here…Insert text here…					
4. The output is in line with the standards adopted by the European Commission.	☐	☐	☐	☐	☐
Insert text here…Insert text here…					

Name of the WP Leader	DTSL - carmel.somers@ictskillnet.ie
Submission Date	[Publish Date]

10. APPENDICES

Appendix A lists the original ENISA Knowledge Area Descriptors

ORIGINAL ENISA KNOWLEDGE DESCRIPTOR	CYBERSECURITY OR SOFT SKILL
Advanced and persistent cyber threats (APT)	Cybersecurity Skill
Auditing standards, methodologies and frameworks	Cybersecurity Skill
Auditing-related certification	Cybersecurity Skill
Computer networks security	Cybersecurity Skill
Computer programming	IT Skill
Computer Security Incident Response Teams (CSIRTs) operation	Cybersecurity Skill
Computer systems vulnerabilities	Cybersecurity Skill
Conformity assessment standards, methodologies and frameworks	Cybersecurity Skill
Criminal investigation procedures, standards, methodologies and frameworks	Cybersecurity Skill
Cross-domain and border-domain knowledge related to cybersecurity	Cybersecurity Skill
Cyber threat actors	Cybersecurity Skill
Cyber Threat Intelligence (CTI) sharing standards, methodologies and frameworks	Cybersecurity Skill
Cyber threats	Cybersecurity Skill

ORIGINAL ENISA KNOWLEDGE DESCRIPTOR	CYBERSECURITY OR SOFT SKILL
Cybersecurity attack procedures	Cybersecurity Skill
Cybersecurity awareness, education and training programme development	Soft Skill
Cybersecurity controls and solutions	Cybersecurity Skill
Cybersecurity education and training standards, methodologies and frameworks	Soft Skill
Cybersecurity maturity models	Cybersecurity Skill
Cybersecurity policies	Cybersecurity Skill
Cybersecurity procedures	Cybersecurity Skill
Cybersecurity recommendations and best practices	IT Skill
Cybersecurity related laws, regulations and legislations	Cybersecurity Skill
Cybersecurity risks	Cybersecurity Skill
Cybersecurity standards, methodologies and frameworks	Cybersecurity Skill
Cybersecurity trends	Soft Skill
Cybersecurity-related certifications	Cybersecurity Skill
Cybersecurity-related requirements analysis	IT Skill

ORIGINAL ENISA KNOWLEDGE DESCRIPTOR	CYBERSECURITY OR SOFT SKILL
Cybersecurity-related research, development and innovation (RDI)	Soft Skill
Cybersecurity-related technologies	Cybersecurity Skill
Digital forensics analysis procedures	Cybersecurity Skill
Digital forensics recommendations and best practices	Cybersecurity Skill
Digital forensics standards, methodologies and frameworks	Cybersecurity Skill
Ethical cybersecurity organisation requirements	Cybersecurity Skill
Incident handling communication procedures	Cybersecurity Skill
Incident handling recommendations and best practices	Cybersecurity Skill
Incident handling standards, methodologies and frameworks	Cybersecurity Skill
Incident handling tools	Cybersecurity Skill
Information technology (IT) and operational technology (OT) appliances	IT Skill
Legacy cybersecurity procedures	IT Skill
Legal, regulatory and legislative compliance requirements, recommendations and best practices	Cybersecurity Skill

ORIGINAL ENISA KNOWLEDGE DESCRIPTOR	CYBERSECURITY OR SOFT SKILL
Legal, regulatory and legislative requirements on releasing or using cybersecurity related technologies	Cybersecurity Skill
Malware analysis tools	Cybersecurity Skill
Management practices	Soft Skill
Monitoring, testing and evaluating cybersecurity controls' effectiveness	Cybersecurity Skill
Multidiscipline aspect of cybersecurity	Soft Skill
Offensive and defensive security practices	Cybersecurity Skill
Offensive and defensive security procedures	Cybersecurity Skill
Operating systems security	IT Skill
Pedagogical standards, methodologies and frameworks	Soft Skill
Penetration testing procedures	Cybersecurity Skill
Penetration testing standards, methodologies and frameworks	Cybersecurity Skill
Penetration testing tools	Cybersecurity Skill
Privacy impact assessment standards, methodologies and frameworks	Cybersecurity Skill
Privacy-by-design standards, methodologies and frameworks	Cybersecurity Skill

ORIGINAL ENISA KNOWLEDGE DESCRIPTOR	CYBERSECURITY OR SOFT SKILL
Privacy-Enhancing Technologies (PET)	Cybersecurity Skill
Resource management	Soft Skill
Responsible information disclosure procedures	Cybersecurity Skill
Risk management recommendations and best practices	Cybersecurity Skill
Risk management standards, methodologies and frameworks	Cybersecurity Skill
Risk management tools	Cybersecurity Skill
Secure coding recommendations and best practices	IT Skill
Secure development lifecycle	IT Skill
Secure Operation Centres (SOCs) operation	Cybersecurity Skill
Security architecture reference models	IT Skill
Testing procedures	Cybersecurity Skill
Testing standards, methodologies and frameworks	Cybersecurity Skill
Threat actors Tactics, Techniques and Procedures (TTPs)	Cybersecurity Skill

Appendix B: Knowledge Areas by Role and Priority – new knowledge areas identified through the ECSF Review by Academia and Industry in red

Knowledge Area	Role	New Knowledge	Priority
Advanced and persistent cyber threats (APT):	Cyber Threat Intelligence Specialist		Priority 5
Advanced and persistent cyber threats (APT):	Cybersecurity Risk Manager	1	Priority 3
Advanced and persistent cyber threats (APT):	Digital Forensics Investigator	1	Priority 2
Advanced and persistent cyber threats (APT):	Cyber Incident Responder	1	Priority 4
Advanced and persistent cyber threats (APT):	Cybersecurity Implementer	1	Priority 4
Auditing standards, methodologies and frameworks:	Cybersecurity Auditor		Priority 5
Auditing-related certification:	Cybersecurity Auditor		Priority 5
Computer networks security:	Cyber Threat Intelligence Specialist		Priority 3
Computer networks security:	Digital Forensics Investigator		Priority 2
Computer networks security:	Cyber Incident Responder		Priority 5
Computer networks security:	Cybersecurity Implementer		Priority 5
Computer networks security:	Penetration Tester		Priority 5
Computer programming:	Cyber Threat Intelligence Specialist		Priority 3
Computer programming:	Cybersecurity Implementer		Priority 5
Computer programming:	Penetration Tester		Priority 2
Computer Security Incident Response Teams (CSIRTs) Operation	Cyber Threat Intelligence Specialist	1	Priority 1

Knowledge Area	Role	New Knowledge	Priority
Computer Security Incident Response Teams (CSIRTs) Operation	Cyber Incident Responder		Priority 4
Computer Systems Vulnerabilities	Cybersecurity Risk Manager		Priority 4
Computer Systems Vulnerabilities	Digital Forensics Investigator		Priority 1
Computer Systems Vulnerabilities	Cyber Incident Responder		Priority 5
Computer Systems Vulnerabilities	Cybersecurity Researcher	1	Priority 2
Computer Systems Vulnerabilities	Penetration Tester		Priority 5
Computer Systems Vulnerabilities	Cybersecurity Implementer	1	Priority 5
Criminal investigation procedures, standards, methodologies, and frameworks:	Digital Forensics Investigator		Priority 4
Cross-domain and border-domain knowledge related to cybersecurity:	Cyber Threat Intelligence Specialist		Priority 2
Cross-domain and border-domain knowledge related to cybersecurity:	Cybersecurity Educator		Priority 1
Cross-domain and border-domain knowledge related to cybersecurity:	Cybersecurity Researcher	1	Priority 4
Cyber threat actors:	Cyber Threat Intelligence Specialist		Priority 5
Cyber threat actors:	Cyber Incident Responder	1	Priority 1
Cyber threat actors:	Cybersecurity Implementer	1	Priority 4

Knowledge Area	Role	New Knowledge	Priority
Cyber Threat Intelligence (CTI) sharing standards, methodologies, and frameworks:	Cyber Threat Intelligence Specialist		Priority 5
Cyber Threats	Cyber Threat Intelligence Specialist		Priority 5
Cyber Threats	Cybersecurity Architect		Priority 4
Cyber Threats	Cybersecurity Risk Manager		Priority 4
Cyber Threats	Cyber Incident Responder		Priority 5
Cyber Threats	Digital Forensics Investigator		Priority 1
Cyber Threats	Cybersecurity Implementor	1	Priority 4
Cybersecurity Attack Procedures	Cyber Threat Intelligence Specialist		Priority 5
Cybersecurity Attack Procedures	Digital Forensics Investigator		Priority 3
Cybersecurity Attack Procedures	Cyber Incident Responder		Priority 5
Cybersecurity Attack Procedures	Penetration Tester		Priority 5
Cybersecurity awareness, education, and training programme development:	Cybersecurity Educator		Priority 5
Cybersecurity controls and solutions:	Cyber Threat Intelligence Specialist		Priority 5
Cybersecurity controls and solutions:	Cybersecurity Risk Manager		Priority 4
Cybersecurity controls and solutions:	Cybersecurity Architect		Priority 5
Cybersecurity controls and solutions:	Cybersecurity Implementer		Priority 4
Cybersecurity education and training standards, methodologies, and frameworks:	Cybersecurity Auditor	1	Priority 4

Knowledge Area	Role	New Knowledge	Priority
Cybersecurity education and training standards, methodologies, and frameworks:	Cybersecurity Educator		Priority 4
Cybersecurity maturity models:	CISO		Priority 4
Cybersecurity Knowledge:	CISO		Priority 4
Cybersecurity Knowledge:	Cyber Legal Policy & Compliance Officer		Priority 5
Cybersecurity Procedures	CISO		Priority 5
Cybersecurity Procedures	Cyber Threat Intelligence Specialist	1	Priority 1
Cybersecurity Procedures	Cybersecurity Implementor	1	Priority 4
Cybersecurity Recommendations and Best Practice	CISO		Priority 5
Cybersecurity Recommendations and Best Practice	Cyber Threat Intelligence Specialist	1	Priority 1
Cybersecurity Recommendations and Best Practice	Cybersecurity Educator		Priority 3
Cybersecurity Recommendations and Best Practice	Cybersecurity Implementor		Priority 4
Cybersecurity Recommendations and Best Practice	Cybersecurity Architect		Priority 4
Cybersecurity Recommendations and Best Practice	Penetration Tester	1	Priority 4
Cybersecurity related laws, regulations and legislations:	CISO		Priority 4
Cybersecurity related laws, regulations and legislations:	Cyber Legal Policy & Compliance Officer		Priority 5
Cybersecurity related laws, regulations and legislations:	Cyber Threat Intelligence Specialist	1	Priority 1
Cybersecurity related laws, regulations and legislations:	Cybersecurity Educator	1	Priority 4
Cybersecurity related laws, regulations and legislations:	Digital Forensics Investigator		Priority 4
Cybersecurity related laws, regulations and legislations:	Cyber Incident Responder		Priority 3

Knowledge Area	Role	New Knowledge	Priority
Cybersecurity related laws, regulations and legislations:	Penetration Tester	1	Priority 4
Cybersecurity risks:	Cyber Threat Intelligence Specialist	1	Priority 3
Cybersecurity risks:	Cybersecurity Educator	1	Priority 1
Cybersecurity risks:	Cybersecurity Risk Manager		Priority 5
Cybersecurity risks:	Cybersecurity Architect		Priority 4
Cybersecurity risks:	Cybersecurity Implementer	1	Priority 4
Cybersecurity standards, methodologies and frameworks:	CISO		Priority 5
Cybersecurity standards, methodologies and frameworks:	Cyber Legal Policy & Compliance Officer		Priority 4
Cybersecurity standards, methodologies and frameworks:	Cyber Threat Intelligence Specialist	1	Priority 1
Cybersecurity standards, methodologies and frameworks:	Cybersecurity Auditor		Priority 4
Cybersecurity standards, methodologies and frameworks:	Cybersecurity Educator		Priority 2
Cybersecurity standards, methodologies and frameworks:	Cybersecurity Architect		Priority 5
Cybersecurity standards, methodologies and frameworks:	Cybersecurity Researcher		Priority 2
Cybersecurity trends:	Cyber Threat Intelligence Specialist	1	Priority 4
Cybersecurity trends:	Cybersecurity Educator	1	Priority 1
Cybersecurity trends:	Cyber Incident Responder	1	Priority 1
Cybersecurity trends:	Cybersecurity Architect		Priority 3
Cybersecurity trends:	Cybersecurity Implementer	1	Priority 4
Cybersecurity trends:	Cybersecurity Researcher	1	Priority 5
Cybersecurity-related certifications:	CISO		Priority 4

Knowledge Area	Role	New Knowledge	Priority
Cybersecurity-related certifications:	Cyber Threat Intelligence Specialist		Priority 1
Cybersecurity-related certifications:	Cybersecurity Auditor		Priority 4
Cybersecurity-related certifications:	Cybersecurity Educator		Priority 2
Cybersecurity-related certifications:	Cybersecurity Risk Manager		Priority 1
Cybersecurity-related certifications:	Digital Forensics Investigator		Priority 1
Cybersecurity-related certifications:	Cyber Incident Responder		Priority 1
Cybersecurity-related certifications:	Cybersecurity Architect		Priority 2
Cybersecurity-related certifications:	Penetration Tester		Priority 3
Cybersecurity-related requirements analysis	CISO	1	Priority 4
Cybersecurity-related requirements analysis	Cybersecurity Architect		Priority 5
Cybersecurity-related Research, development and innovation (RDI)	CISO	1	Priority 4
Cybersecurity-related Research, development and innovation (RDI)	Cybersecurity Researcher		Priority 5
Cybersecurity-related technologies:	Cybersecurity Risk Manager		Priority 4
Cybersecurity-related technologies:	Cybersecurity Architect		Priority 3
Cybersecurity-related technologies:	Cybersecurity Implementer		Priority 5
Digital forensics analysis procedures:	Digital Forensics Investigator		Priority 5
Digital forensics recommendations and best practices:	Digital Forensics Investigator		Priority 5
Digital forensics standards, methodologies and frameworks:	Digital Forensics Investigator		Priority 4

Knowledge Area	Role	New Knowledge	Priority
Ethical cybersecurity organisation requirements:	CISO		Priority 4
Ethical cybersecurity organisation requirements:	Cybersecurity Educator	1	Priority 4
Ethical cybersecurity organisation requirements:	Penetration Tester	1	Priority 4
Incident handling communication procedures:	CISO	1	Priority 1
Incident handling communication procedures:	Cyber Incident Responder		Priority 5
Incident handling communication procedures:	Cybersecurity Researcher		Priority 5
Incident Handling Recommendations and Best Practices	CISO	1	Priority 1
Incident Handling Recommendations and Best Practices	Cyber Incident Responder		Priority 4
Incident Handling Standards, Methodologies and Frameworks	Cyber Threat Intelligence Specialist	1	Priority 3
Incident Handling Standards, Methodologies and Frameworks	Cyber Incident Responder		Priority 4
Incident Handling Tools	Cyber Threat Intelligence Specialist	1	Priority 4
Incident Handling Tools	Cyber Incident Responder		Priority 4
Information technology (IT) and operational technology (OT) appliances:	Penetration Tester		Priority 4
Legacy cybersecurity procedures:	Cyber Threat Intelligence Specialist	1	Priority 1
Legacy cybersecurity procedures:	Cybersecurity Architect		Priority 2
Legal, regulatory and legislative compliance requirements, recommendations and best practices:	Cybersecurity Auditor		Priority 5
Legal, regulatory and legislative compliance requirements, recommendations and best practices:	Cybersecurity Educator		Priority 2

Knowledge Area	Role	New Knowledge	Priority
Legal, regulatory and legislative compliance requirements, recommendations and best practices:	Cyber Incident Responder	1	Priority 4
Legal, regulatory and legislative compliance requirements, recommendations and best practices:	Digital Forensics Investigator	1	Priority 4
Legal, regulatory and legislative compliance requirements, recommendations and best practices:	Cybersecurity Architect		Priority 4
Legal, regulatory and legislative requirements on releasing or using cybersecurity-related technologies:	Cyber Legal Policy & Compliance Officer		Priority 5
Legal, regulatory and legislative requirements on releasing or using cybersecurity-related technologies:	Cyber Threat Intelligence Specialist	1	Priority 1
Legal, regulatory and legislative requirements on releasing or using cybersecurity-related technologies:	Cyber Incident Responder	1	Priority 4
Legal, regulatory and legislative requirements on releasing or using cybersecurity-related technologies:	Cybersecurity Researcher		Priority 2
Malware analysis tools:	Digital Forensics Investigator		Priority 5
Management practices:	CISO		Priority 4
Monitoring, testing and evaluating cybersecurity controls' effectiveness:	Cybersecurity Auditor		Priority 4
Monitoring, testing and evaluating cybersecurity controls' effectiveness:	Cybersecurity Risk Manager		Priority 3

Knowledge Area	Role	New Knowledge	Priority
Monitoring, testing and evaluating cybersecurity controls' effectiveness:	Penetration Tester	1	Priority 4
Multidiscipline aspect of cybersecurity:	CISO	1	Priority 4
Multidiscipline aspect of cybersecurity:	Cyber Threat Intelligence Specialist	1	Priority 4
Multidiscipline aspect of cybersecurity:	Cybersecurity Educator	1	Priority 2
Multidiscipline aspect of cybersecurity:	Cybersecurity Researcher		Priority 3
Offensive and defensive security practices:	Cyber Threat Intelligence Specialist	1	Priority 2
Offensive and defensive security practices:	Digital Forensics Investigator	1	Priority 1
Offensive and defensive security practices:	Cybersecurity Implementer		Priority 4
Offensive and defensive security practices:	Penetration Tester		Priority 4
Offensive and defensive security procedures:	Cyber Threat Intelligence Specialist	1	Priority 3
Offensive and defensive security procedures:	Penetration Tester	1	Priority 5
Operating Systems Security	Cyber Threat Intelligence Specialist		Priority 5
Operating Systems Security	Cybersecurity Educator	1	Priority 1
Operating Systems Security	Digital Forensics Investigator		Priority 4
Operating Systems Security	Cyber Incident Responder		Priority 3
Operating Systems Security	Cybersecurity Implementer		Priority 4
Operating Systems Security	Penetration Tester		Priority 4
Pedagogical standards, methodologies and frameworks:	Cybersecurity Educator		Priority 3
Penetration testing procedures:	Penetration Tester		Priority 5

Knowledge Area	Role	New Knowledge	Priority
Penetration testing standards, methodologies and frameworks:	Penetration Tester		Priority 5
Penetration testing tools:	Penetration Tester		Priority 5
Privacy impact assessment standards, methodologies and frameworks:	Cyber Legal Policy & Compliance Officer		Priority 4
Privacy-by-design standards, methodologies and frameworks:	Cyber Legal Policy & Compliance Officer	1	Priority 4
Privacy-by-design standards, methodologies and frameworks:	Cybersecurity Architect		Priority 5
Privacy-Enhancing Technologies (PET):	Cybersecurity Architect		Priority 3
Resource management:	CISO		Priority 4
Responsible information disclosure procedures:	Cyber Threat Intelligence Specialist		Priority 3
Responsible information disclosure procedures:	Digital Forensics Investigator	1	Priority 1
Responsible information disclosure procedures:	Cyber Incident Responder	1	Priority 1
Responsible information disclosure procedures:	Cybersecurity Researcher		Priority 2
Risk management recommendations and best practices:	Cyber Threat Intelligence Specialist	1	Priority 3
Risk management recommendations and best practices:	Cybersecurity Auditor	1	Priority 4
Risk management recommendations and best practices:	Cybersecurity Risk Manager		Priority 5
Risk management recommendations and best practices:	Cyber Incident Responder	1	Priority 4
Risk management standards, methodologies and frameworks:	CISO		Priority 5

Knowledge Area	Role	New Knowledge	Priority
Risk management standards, methodologies and frameworks:	Cyber Threat Intelligence Specialist	1	Priority 3
Risk management standards, methodologies and frameworks:	Cybersecurity Risk Manager		Priority 5
Risk management standards, methodologies and frameworks:	Digital Forensics Investigator	1	Priority 1
Risk management standards, methodologies and frameworks:	Cyber Incident Responder		Priority 4
Risk management tools:	Cyber Threat Intelligence Specialist	1	Priority 3
Risk management tools:	Cybersecurity Risk Manager		Priority 5
Risk management tools:	Cyber Incident Responder		Priority 4
Secure coding recommendations and best practices:	Cybersecurity Implementer		Priority 5
Secure development lifecycle:	Cybersecurity Architect		Priority 4
Secure development lifecycle:	Cybersecurity Implementer		Priority 4
Secure Operation Centres (SOCs) operation:	Cyber Threat Intelligence Specialist	1	Priority 3
Secure Operation Centres (SOCs) operation:	Digital Forensics Investigator	1	Priority 1
Secure Operation Centres (SOCs) operation:	Cyber Incident Responder		Priority 4
Security architecture reference models:	Cyber Threat Intelligence Specialist	1	Priority 3
Security architecture reference models:	Cybersecurity Architect		Priority 4
Testing procedures:	Digital Forensics Investigator		Priority 1

Knowledge Area	Role	New Knowledge	Priority
Testing procedures:	Cybersecurity Implementer		Priority 5
Testing standards, methodologies and frameworks:	Cybersecurity Implementer		Priority 5
Testing standards, methodologies and frameworks:	Digital Forensics Investigator	1	Priority 1
Threat actors Tactics, Techniques and Procedures (TTPs):	Cyber Threat Intelligence Specialist		Priority 5
Threat actors Tactics, Techniques and Procedures (TTPs):	Digital Forensics Investigator	1	Priority 4
Cloud Security Specific Knowledge	Penetration Tester	1	Priority 4
Other Forensics Skills	Digital Forensics Investigator	1	Priority 4

Appendix C: New Knowledge Areas by Role in order of Priority (5 High to 1 Low)

Knowledge Area	Role	New Knowledge	Priority
Computer Systems Vulnerabilities	Cybersecurity Implementer	1	Priority 5
Cybersecurity trends:	Cybersecurity Researcher	1	Priority 5
Offensive and defensive security procedures:	Penetration Tester	1	Priority 5
Advanced and persistent cyber threats (APT):	Cyber Incident Responder	1	Priority 4
Advanced and persistent cyber threats (APT):	Cybersecurity Implementer	1	Priority 4
Cross-domain and border-domain knowledge related to cybersecurity:	Cybersecurity Researcher	1	Priority 4
Cyber threat actors:	Cybersecurity Implementer	1	Priority 4
Cyber Threats	Cybersecurity Implementor	1	Priority 4
Cybersecurity education and training standards, methodologies, and frameworks:	Cybersecurity Auditor	1	Priority 4
Cybersecurity Procedures	Cybersecurity Implementor	1	Priority 4
Cybersecurity Recommendations and Best Practice	Penetration Tester	1	Priority 4
Cybersecurity related laws, regulations and legislations:	Cybersecurity Educator	1	Priority 4
Cybersecurity related laws, regulations and legislations:	Penetration Tester	1	Priority 4
Cybersecurity risks:	Cybersecurity Implementer	1	Priority 4
Cybersecurity trends:	Cyber Threat Intelligence Specialist	1	Priority 4

Knowledge Area	Role	New Knowledge	Priority
Cybersecurity trends:	Cybersecurity Implementer	1	Priority 4
Cybersecurity-related requirements analysis	CISO	1	Priority 4
Cybersecurity-related Research, development and innovation (RDI)	CISO	1	Priority 4
Ethical cybersecurity organisation requirements:	Cybersecurity Educator	1	Priority 4
Ethical cybersecurity organisation requirements:	Penetration Tester	1	Priority 4
Incident Handling Tools	Cyber Threat Intelligence Specialist	1	Priority 4
Legal, regulatory and legislative compliance requirements, recommendations and best practices:	Cyber Incident Responder	1	Priority 4
Legal, regulatory and legislative compliance requirements, recommendations and best practices:	Digital Forensics Investigator	1	Priority 4
Legal, regulatory and legislative requirements on releasing or using cybersecurity-related technologies:	Cyber Incident Responder	1	Priority 4
Monitoring, testing and evaluating cybersecurity controls' effectiveness:	Penetration Tester	1	Priority 4
Multidiscipline aspect of cybersecurity:	CISO	1	Priority 4
Multidiscipline aspect of cybersecurity:	Cyber Threat Intelligence Specialist	1	Priority 4
Privacy-by-design standards, methodologies and frameworks:	Cyber Legal Policy & Compliance Officer	1	Priority 4
Risk management recommendations and best practices:	Cybersecurity Auditor	1	Priority 4
Risk management recommendations and best practices:	Cyber Incident Responder	1	Priority 4

Knowledge Area	Role	New Knowledge	Priority
Threat actors Tactics, Techniques and Procedures (TTPs):	Digital Forensics Investigator	1	Priority 4
Cloud Security Specific Knowledge	Penetration Tester	1	Priority 4
Other Forensics Skills	Digital Forensics Investigator	1	Priority 4
Advanced and persistent cyber threats (APT):	Cybersecurity Risk Manager	1	Priority 3
Cybersecurity risks:	Cyber Threat Intelligence Specialist	1	Priority 3
Incident Handling Standards, Methodologies and Frameworks	Cyber Threat Intelligence Specialist	1	Priority 3
Offensive and defensive security procedures:	Cyber Threat Intelligence Specialist	1	Priority 3
Risk management recommendations and best practices:	Cyber Threat Intelligence Specialist	1	Priority 3
Risk management standards, methodologies and frameworks:	Cyber Threat Intelligence Specialist	1	Priority 3
Risk management tools:	Cyber Threat Intelligence Specialist	1	Priority 3
Secure Operation Centres (SOCs) operation:	Cyber Threat Intelligence Specialist	1	Priority 3
Security architecture reference models:	Cyber Threat Intelligence Specialist	1	Priority 3
Advanced and persistent cyber threats (APT):	Digital Forensics Investigator	1	Priority 2
Computer Systems Vulnerabilities	Cybersecurity Researcher	1	Priority 2
Multidiscipline aspect of cybersecurity:	Cybersecurity Educator	1	Priority 2
Offensive and defensive security practices:	Cyber Threat Intelligence Specialist	1	Priority 2
Computer Security Incident Response Teams (CSIRTs) Operation	Cyber Threat Intelligence Specialist	1	Priority 1
Cyber threat actors:	Cyber Incident Responder	1	Priority 1

Knowledge Area	Role	New Knowledge	Priority
Cybersecurity Procedures	Cyber Threat Intelligence Specialist	1	Priority 1
Cybersecurity Recommendations and Best Practice	Cyber Threat Intelligence Specialist	1	Priority 1
Cybersecurity related laws, regulations and legislations:	Cyber Threat Intelligence Specialist	1	Priority 1
Cybersecurity risks:	Cybersecurity Educator	1	Priority 1
Cybersecurity standards, methodologies and frameworks:	Cyber Threat Intelligence Specialist	1	Priority 1
Cybersecurity trends:	Cybersecurity Educator	1	Priority 1
Cybersecurity trends:	Cyber Incident Responder	1	Priority 1
Incident handling communication procedures:	CISO	1	Priority 1
Incident Handling Recommendations and Best Practices	CISO	1	Priority 1
Legacy cybersecurity procedures:	Cyber Threat Intelligence Specialist	1	Priority 1
Legal, regulatory and legislative requirements on releasing or using cybersecurity-related technologies:	Cyber Threat Intelligence Specialist	1	Priority 1
Offensive and defensive security practices:	Digital Forensics Investigator	1	Priority 1
Operating Systems Security	Cybersecurity Educator	1	Priority 1
Responsible information disclosure procedures:	Digital Forensics Investigator	1	Priority 1
Responsible information disclosure procedures:	Cyber Incident Responder	1	Priority 1
Risk management standards, methodologies and frameworks:	Digital Forensics Investigator	1	Priority 1
Secure Operation Centres (SOCs) operation:	Digital Forensics Investigator	1	Priority 1
Testing standards, methodologies and frameworks:	Digital Forensics Investigator	1	Priority 1

Appendix D: The original ENISA Skill Descriptors

Original ENISA Skill Descriptor	Category
Anticipate cybersecurity threats, needs and upcoming challenges	Soft Skill
Anticipate required changes to the organisation's information security strategy and formulate new plans	Soft Skill
Apply auditing tools and techniques	Cybersecurity Skill
Assess and enhance an organisation's cybersecurity posture	Cybersecurity Skill
Assess the security and performance of solutions	Cybersecurity Skill
Audit with integrity, being impartial and independent	Cybersecurity Skill
Automate threat intelligence management procedures	Cybersecurity Skill
Build a cybersecurity risk-aware environment	Soft Skill
Build resilience against points of failure across the architecture	IT Skill
Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy	Cybersecurity Skill
Collaborate with other team members and colleagues	Soft Skill
Collect information while preserving its integrity	Cybersecurity Skill
Collect, analyse and correlate cyber threat information originating from multiple sources	Cybersecurity Skill
Collect, evaluate, maintain and protect auditing information	Cybersecurity Skill
Communicate, coordinate and cooperate with internal and external stakeholders	Soft Skill
Communicate, explain and adapt legal and regulatory requirements and business needs	Cybersecurity Skill
Communicate, present and report to relevant stakeholders	Soft Skill

Original ENISA Skill Descriptor	Category
Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements	Cybersecurity Skill
Conduct ethical hacking	Cybersecurity Skill
Conduct technical analysis and reporting	Cybersecurity Skill
Conduct user and business security requirements analysis	IT Skill
Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools	Cybersecurity Skill
Configure solutions according to the organisation's security policy	IT Skill
Coordinate the integration of security solutions	IT Skill
Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	IT Skill
Decompose and analyse systems to identify weaknesses and ineffective controls	IT Skill
Define and apply maturity models for cybersecurity management	Cybersecurity Skill
Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles	IT Skill
Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing	Soft Skill
Design, develop and deliver learning programmes to cover cybersecurity needs	Soft Skill
Develop and communicate, detailed and reasoned investigation reports	Soft Skill
Develop code, scripts and programmes	Cybersecurity Skill
Develop cybersecurity exercises including simulations using cyber range environments	Soft Skill
Develop evaluation programs for the awareness, training and education activities	Soft Skill

Original ENISA Skill Descriptor	Category
Develop, champion and lead the execution of a cybersecurity strategy	Soft Skill
Draw cybersecurity architectural and functional specifications	IT Skill
Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks	Cybersecurity Skill
Establish a cybersecurity plan	Soft Skill
Explain and communicate data protection and privacy topics to stakeholders and users	Cybersecurity Skill
Explain and present digital evidence in a simple, straightforward and easy to understand way	Cybersecurity Skill
Follow and practice auditing frameworks, standards and methodologies	Cybersecurity Skill
Generate new ideas and transfer theory into practice	Soft Skill
Guide and communicate with implementers and IT/OT personnel	Soft Skill
Identify and exploit vulnerabilities	Cybersecurity Skill
Identify and select appropriate pedagogical approaches for the intended audience	Soft Skill
Identify and solve cybersecurity-related issues	Cybersecurity Skill
Identify needs in cybersecurity awareness, training and education	Soft Skill
Identify non-cyber events with implications on cyber-related activities	Cybersecurity Skill
Identify threat actors TTPs and campaigns	Cybersecurity Skill
Identify, analyse and correlate cybersecurity events	Cybersecurity Skill
Implement cybersecurity recommendations and best practices	IT Skill
Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards	Cybersecurity Skill

Original ENISA Skill Descriptor	Category
Influence an organisation's cybersecurity culture	Soft Skill
Integrate cybersecurity solutions to the organisation's infrastructure	IT Skill
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	Cybersecurity Skill
Manage and analyse log files	Cybersecurity Skill
Manage cybersecurity resources	IT Skill
Model threats, actors and TTPs	Cybersecurity Skill
Monitor new advancements in cybersecurity-related technologies	Soft Skill
Motivate and encourage people	Soft Skill
Organise and work in a systematic and deterministic way based on evidence	Cybersecurity Skill
Perform social engineering	Cybersecurity Skill
Practice all technical, functional and operational aspects of cybersecurity incident handling and response	Cybersecurity Skill
Propose and manage risk-sharing options	Cybersecurity Skill
Propose cybersecurity architectures based on stakeholder's needs and budget	IT Skill
Provide training towards cybersecurity and data protection professional certifications	Soft Skill
Review and enhance security documents, reports, SLAs and ensure the security objectives	Soft Skill
Review codes assess their security	IT Skill
Select appropriate specifications, procedures and controls	IT Skill

Original ENISA Skill Descriptor	Category
Think creatively and outside the box	Soft Skill
Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies	Cybersecurity Skill
Understand, practice and adhere to ethical requirements and standards	Cybersecurity Skill
Use and apply CTI platforms and tools	Cybersecurity Skill
Use penetration testing tools effectively	Cybersecurity Skill
Utilise existing cybersecurity-related training resources	Soft Skill
Work ethically and independently; not influenced and biased by internal or external actors	Cybersecurity Skill
Work on operating systems, servers, clouds and relevant infrastructures	IT Skill
Work under pressure	Soft Skill

Appendix E: Skills by Role and Priority – new skills identified through the ECSF Review by Academia and Industry in red

Skills Areas	Role	New Skill	Priority
Anticipate cybersecurity threats, needs and upcoming challenges	CISO		Priority 5
Anticipate cybersecurity threats, needs and upcoming challenges	Cybersecurity Architect	1	Priority 4
Anticipate cybersecurity threats, needs and upcoming challenges	Cybersecurity Auditor	1	Priority 5
Anticipate cybersecurity threats, needs and upcoming challenges	Cybersecurity Researcher	1	Priority 2
Anticipate required changes to the organisation's information security strategy and formulate new plans	CISO		Priority 4
Anticipate required changes to the organisation's information security strategy and formulate new plans	Cybersecurity Architect	1	Priority 4
Apply auditing tools and techniques	Cyber Threat intelligence Specialist	1	Priority 4
Apply auditing tools and techniques	Cybersecurity Auditor		Priority 5
Apply auditing tools and techniques	Cybersecurity Architect	1	Priority 4
Assess and enhance an organisation's cybersecurity posture	CISO		Priority 3
Assess the security and performance of solutions	CISO	1	Priority 4
Assess the security and performance of solutions	Cybersecurity Architect	1	Priority 4

Skills Areas	Role	New Skill	Priority
Assess the security and performance of solutions	Cybersecurity Implementor		Priority 4
Assess the security and performance of solutions	Penetration Tester	1	Priority 3
Audit with Integrity, being impartial and independent	CISO	1	Priority 4
Audit with Integrity, being impartial and independent	Cybersecurity Auditor		Priority 5
Audit with Integrity, being impartial and independent	Cyber Threat intelligence Specialist	1	Priority 5
Automate Threat intelligence management Procedures	Cyber Threat intelligence Specialist		Priority 4
Build a cybersecurity risk-aware environment	Cybersecurity Risk Manager		Priority 5
Build resilience against points of failure across the architecture	Cybersecurity Architect		Priority 5
Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy	Cyber Legal Policy & Compliance Officer		Priority 4
Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy	Cybersecurity Implementor	1	Priority 4
Collaborate with other team members and colleagues	Cybersecurity Auditor	1	Priority 3
Collaborate with other team members and colleagues	Cybersecurity Implementor		Priority 4
Collaborate with other team members and colleagues	Cyber Legal Policy & Compliance Officer		Priority 4
Collaborate with other team members and colleagues	Cyber Threat intelligence Specialist		Priority 3
Collaborate with other team members and colleagues	Cybersecurity Architect	1	Priority 4
Collaborate with other team members and colleagues	Cybersecurity Researcher		Priority 3
Collect information while preserving its integrity	Digital Forensics Investigator		Priority 5

Skills Areas	Role	New Skill	Priority
Collect information while preserving its integrity	Penetration Tester	1	Priority 4
Collect, analyse and correlate cyber threat information originating from multiple sources	CISO	1	Priority 4
Collect, analyse and correlate cyber threat information originating from multiple sources	Cyber Threat intelligence Specialist		Priority 5
Collect, analyse and correlate cyber threat information originating from multiple sources	Cyber Incident Responder		Priority 4
Collect, analyse and correlate cyber threat information originating from multiple sources	Penetration Tester	1	Priority 4
Collect, evaluate, maintain and protect auditing information	Cyber Threat intelligence Specialist	1	Priority 4
Collect, evaluate, maintain and protect auditing information	Cybersecurity Auditor		Priority 5
Collect, evaluate, maintain and protect auditing information	Digital Forensics Investigator	1	Priority 2
Communicate, coordinate and cooperate with internal and external stakeholders	CISO		Priority 5
Communicate, coordinate and cooperate with internal and external stakeholders	Cyber Threat intelligence Specialist		Priority 2
Communicate, coordinate and cooperate with internal and external stakeholders	Cybersecurity Auditor	1	Priority 4
Communicate, coordinate and cooperate with internal and external stakeholders	Digital Forensics Investigator	1	Priority 3

Skills Areas	Role	New Skill	Priority
Communicate, coordinate and cooperate with internal and external stakeholders	Cybersecurity Architect	1	Priority 4
Communicate, coordinate and cooperate with internal and external stakeholders	Penetration Tester	1	Priority 4
Communicate, explain and adapt legal and regulatory requirements and business needs	Cybersecurity Auditor		Priority 5
Communicate, present and report to relevant stakeholders	Cyber Threat intelligence Specialist		Priority 3
Communicate, present and report to relevant stakeholders	Cyber Incident Responder		Priority 4
Communicate, present and report to relevant stakeholders	Cybersecurity Implementor		Priority 4
Communicate, present and report to relevant stakeholders	Cybersecurity Risk Manager		Priority 2
Communicate, present and report to relevant stakeholders	Cybersecurity Educator		Priority 4
Communicate, present and report to relevant stakeholders	Cybersecurity Auditor	1	Priority 4
Communicate, present and report to relevant stakeholders	Digital Forensics Investigator	1	Priority 3
Communicate, present and report to relevant stakeholders	Cybersecurity Architect		Priority 3
Communicate, present and report to relevant stakeholders	Cybersecurity Researcher		Priority 4
Communicate, present and report to relevant stakeholders	Penetration Tester		Priority 4
Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements	Cyber Legal Policy & Compliance Officer		Priority 4

Skills Areas	Role	New Skill	Priority
Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements	Cybersecurity Auditor	1	Priority 4
Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements	Cybersecurity Architect	1	Priority 4
Conduct ethical hacking	Penetration Tester		Priority 5
Conduct technical analysis and reporting	Cyber Threat intelligence Specialist		Priority 5
Conduct technical analysis and reporting	Cybersecurity Implementor	1	Priority 4
Conduct technical analysis and reporting	Penetration Tester		Priority 4
Conduct user and business security requirements analysis	Cybersecurity Architect		Priority 5
Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools	Cyber Legal Policy & Compliance Officer		Priority 5
Configure solutions according to the organisation's security policy	Cybersecurity Implementor		Priority 5
Coordinate the integration of security solutions	Cybersecurity Architect		Priority 4
Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Cybersecurity Architect		Priority 5
Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Cyber Incident Responder	1	Priority 5
Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Cybersecurity Researcher		Priority 2

Skills Areas	Role	New Skill	Priority
Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Cybersecurity Auditor		Priority 4
Decompose and analyse systems to identify weaknesses and ineffective controls	Cyber Threat Intelligence Specialist	1	Priority 5
Decompose and analyse systems to identify weaknesses and ineffective controls	Cybersecurity Researcher		Priority 2
Decompose and analyse systems to identify weaknesses and ineffective controls	Penetration Tester		Priority 4
Define and apply maturity models for cybersecurity management	CISO		Priority 5
Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles	Cybersecurity Architect		Priority 5
Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles	Cybersecurity Researcher	1	Priority 2
Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing	CISO		Priority 5
Design, develop and deliver learning programmes to cover cybersecurity needs	Cybersecurity Educator		Priority 4
Develop and communicate, detailed and reasoned investigation reports	Cyber Threat Intelligence Specialist	1	Priority 2

Skills Areas	Role	New Skill	Priority
Develop and communicate, detailed and reasoned investigation reports	Digital Forensics Investigator		Priority 4
Develop and communicate, detailed and reasoned investigation reports	Penetration Tester	1	Priority 4
Develop code, scripts and programmes	Cybersecurity Implementor		Priority 4
Develop code, scripts and programmes	Penetration Tester		Priority 3
Develop cybersecurity exercises including simulations using cyber range environments	Cybersecurity Educator		Priority 4
Develop evaluation programs for the awareness, training and education activities	Cybersecurity Educator		Priority 4
Develop, champion and lead the execution of a cybersecurity strategy	CISO		Priority 5
Draw cybersecurity architectural and functional specifications	Cybersecurity Architect		Priority 4
Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks	Cybersecurity Risk Manager		Priority 4
Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks	CISO	1	Priority 4
Establish a cybersecurity plan	CISO		Priority 5

Skills Areas	Role	New Skill	Priority
Explain and communicate data protection and privacy topics to stakeholders and users	Cyber Legal Policy & Compliance Officer		Priority 3
Explain and present digital evidence in a simple, straightforward and easy to understand way	Digital Forensics Investigator		Priority 5
Follow and practice auditing frameworks, standards and methodologies	CISO	1	Priority 4
Follow and practice auditing frameworks, standards and methodologies	Cybersecurity Auditor		Priority 4
Follow and practice auditing frameworks, standards and methodologies	Cyber Threat Intelligence Specialist	1	Priority 5
Generate new ideas and transfer theory into practice	Cybersecurity Researcher		Priority 5
Guide and communicate with implementers and IT/OT personnel	Cybersecurity Implementor	1	Priority 4
Guide and communicate with implementers and IT/OT personnel	Cybersecurity Architect		Priority 4
Identify and exploit vulnerabilities	Cyber Threat Intelligence Specialist	1	Priority 4
Identify and exploit vulnerabilities	Cybersecurity Implementor	1	Priority 4
Identify and exploit vulnerabilities	Penetration Tester		Priority 5
Identify and select appropriate pedagogical approaches for the intended audience	Cybersecurity Educator		Priority 4
Identify and solve cybersecurity-related issues	CISO		Priority 3
Identify and solve cybersecurity-related issues	Cyber Threat Intelligence Specialist	1	Priority 2
Identify and solve cybersecurity-related issues	Cybersecurity Educator		Priority 2

Skills Areas	Role	New Skill	Priority
Identify and solve cybersecurity-related issues	Cybersecurity Architect	1	Priority 4
Identify and solve cybersecurity-related issues	Cybersecurity Implementor		Priority 4
Identify and solve cybersecurity-related issues	Cybersecurity Researcher		Priority 3
Identify and solve cybersecurity-related issues	Penetration Tester		Priority 3
Identify needs in cybersecurity awareness, training and education	Cybersecurity Educator		Priority 3
Identify needs in cybersecurity awareness, training and education	Cybersecurity Auditor	1	Priority 4
Identify non-cyber events with implications on cyber-related activities	Cyber Threat Intelligence Specialist		Priority 5
Identify threat actors TTPs and campaigns	Cyber Threat Intelligence Specialist		Priority 5
Identify threat actors TTPs and campaigns	Cyber Incident Responder	1	Priority 4
Identify, analyse and correlate cybersecurity events	Cyber Threat Intelligence Specialist	1	Priority 4
Identify, analyse and correlate cybersecurity events	Digital Forensics Investigator		Priority 2
Implement cybersecurity recommendations and best practices	CISO		Priority 3
Implement cybersecurity recommendations and best practices	Cybersecurity Researcher	1	Priority 2
Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards	Cybersecurity Risk Manager		Priority 5
Influence an organisation's cybersecurity culture	CISO		Priority 4
Influence an organisation's cybersecurity culture	Cybersecurity Architect	1	Priority 4
Integrate cybersecurity solutions to the organisation's infrastructure	CISO	1	Priority 4

Skills Areas	Role	New Skill	Priority
Integrate cybersecurity solutions to the organisation's infrastructure	Cybersecurity Architect	1	Priority 4
Integrate cybersecurity solutions to the organisation's infrastructure	Cybersecurity Implementor		Priority 4
Integrate cybersecurity solutions to the organisation's infrastructure	Cybersecurity Researcher	1	Priority 4
Lead the development of appropriate cybersecurity and privacy policies and procedures	Cyber Legal Policy & Compliance Officer		Priority 5
Manage and analyse log files	Cyber Incident Responder		Priority 4
Manage and analyse log files	Penetration Tester	1	Priority 4
Manage cybersecurity resources	CISO		Priority 4
Model threats, actors and TTPs	Cyber Threat Intelligence Specialist		Priority 4
Monitor new advancements in cybersecurity-related technologies	Cyber Threat Intelligence Specialist	1	Priority 1
Monitor new advancements in cybersecurity-related technologies	Digital Forensics Investigator	1	Priority 3
Monitor new advancements in cybersecurity-related technologies	Cybersecurity Researcher		Priority 4
Monitor new advancements in cybersecurity-related technologies	Penetration Tester		Priority 4
Motivate and encourage people	CISO		Priority 4
Motivate and encourage people	Cybersecurity Educator		Priority 4
Organise and work in a systematic and deterministic way based on evidence	Cybersecurity Auditor		Priority 5

Skills Areas	Role	New Skill	Priority
Organise and work in a systematic and deterministic way based on evidence	Digital Forensics Investigator	1	Priority 4
Perform social engineering	Cyber Threat Intelligence Specialist	1	Priority 4
Perform social engineering	Penetration Tester		Priority 4
Practice all technical, functional and operational aspects of cybersecurity incident handling and response	Cyber Incident Responder		Priority 5
Practice all technical, functional and operational aspects of cybersecurity incident handling and response	Penetration Tester	1	Priority 4
Propose and manage risk-sharing options	Cybersecurity Risk Manager		Priority 3
Propose cybersecurity architectures based on stakeholder's needs and budget	Cybersecurity Architect		Priority 4
Provide training towards cybersecurity and data protection professional certifications	CISO	1	Priority 4
Provide training towards cybersecurity and data protection professional certifications	Cybersecurity Educator		Priority 3
Review and enhance security documents, reports, SLAs and ensure the security objectives	CISO		Priority 5
Review codes assess their security	Penetration Tester		Priority 3
Select appropriate specifications, procedures and controls	Cybersecurity Architect		Priority 5
Think creatively and outside the box	Cyber Threat Intelligence Specialist	1	Priority 2
Think creatively and outside the box	Cybersecurity Researcher	1	Priority 4

Skills Areas	Role	New Skill	Priority
Think creatively and outside the box	Cyber Incident Responder	1	Priority 2
Think creatively and outside the box	Penetration Tester	1	Priority 4
Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies	Cyber Legal Policy & Compliance Officer		Priority 5
Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies	Cybersecurity Auditor	1	Priority 4
Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies	Cybersecurity Architect	1	Priority 4
Understand, practice and adhere to ethical requirements and standards	Cyber Legal Policy & Compliance Officer		Priority 5
Use and apply CTI platforms and tools	Cyber Threat Intelligence Specialist		Priority 4
Use and apply CTI platforms and tools	Penetration Tester	1	Priority 4
Use penetration testing tools effectively	Penetration Tester		Priority 5
Utilise existing cybersecurity-related training resources	Cybersecurity Educator		Priority 4
Work ethically and independently; not influenced and biased by internal or external actors	Digital Forensics Investigator		Priority 4
Work ethically and independently; not influenced and biased by internal or external actors	Cybersecurity Auditor	1	Priority 4

Skills Areas	Role	New Skill	Priority
Work ethically and independently; not influenced and biased by internal or external actors	Penetration Tester		Priority 4
Work on operating systems, servers, clouds and relevant infrastructures	Cyber Incident Responder		Priority 5
Work on operating systems, servers, clouds and relevant infrastructures	Digital Forensics Investigator	1	Priority 3
Work under pressure	Digital Forensics Investigator	1	Priority 1
Work under pressure	Cyber Incident Responder		Priority 5
Stakeholder management	CISO	1	Priority 4
Change management	Cyber Threat Intelligence Specialist	1	Priority 4
Certifications	Cyber Threat Intelligence Specialist	1	Priority 4
Technical Proficiency	Cyber Threat Intelligence Specialist	1	Priority 4
Incident Response	Cyber Threat Intelligence Specialist	1	Priority 4
Continuous Learning	Cyber Threat Intelligence Specialist	1	Priority 4
Continuous Learning	Cyber Threat Intelligence Specialist	1	Priority 4

APPENDIX F: New Skill Areas by Role in order of Priority (5 High to 1 Low)

Skills Areas	Role	New Skill	Priority
Anticipate cybersecurity threats, needs and upcoming challenges	Cybersecurity Auditor	1	Priority 5
Audit with Integrity, being impartial and independent	Cyber Threat intelligence Specialist	1	Priority 5
Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Cyber Incident Responder	1	Priority 5
Decompose and analyse systems to identify weaknesses and ineffective controls	Cyber Threat Intelligence Specialist	1	Priority 5
Follow and practice auditing frameworks, standards and methodologies	Cyber Threat Intelligence Specialist	1	Priority 5
Anticipate cybersecurity threats, needs and upcoming challenges	Cybersecurity Architect	1	Priority 4
Anticipate required changes to the organisation's information security strategy and formulate new plans	Cybersecurity Architect	1	Priority 4
Apply auditing tools and techniques	Cyber Threat intelligence Specialist	1	Priority 4
Apply auditing tools and techniques	Cybersecurity Architect	1	Priority 4
Assess the security and performance of solutions	CISO	1	Priority 4
Assess the security and performance of solutions	Cybersecurity Architect	1	Priority 4
Audit with Integrity, being impartial and independent	CISO	1	Priority 4

Skills Areas	Role	New Skill	Priority
Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy	Cybersecurity Implementor	1	Priority 4
Collaborate with other team members and colleagues	Cybersecurity Architect	1	Priority 4
Collect information while preserving its integrity	Penetration Tester	1	Priority 4
Collect, analyse and correlate cyber threat information originating from multiple sources	CISO	1	Priority 4
Collect, analyse and correlate cyber threat information originating from multiple sources	Penetration Tester	1	Priority 4
Collect, evaluate, maintain and protect auditing information	Cyber Threat intelligence Specialist	1	Priority 4
Communicate, coordinate and cooperate with internal and external stakeholders	Cybersecurity Auditor	1	Priority 4
Communicate, coordinate and cooperate with internal and external stakeholders	Cybersecurity Architect	1	Priority 4
Communicate, coordinate and cooperate with internal and external stakeholders	Penetration Tester	1	Priority 4
Communicate, present and report to relevant stakeholders	Cybersecurity Auditor	1	Priority 4
Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements	Cybersecurity Auditor	1	Priority 4

Skills Areas	Role	New Skill	Priority
Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements	Cybersecurity Architect	1	Priority 4
Conduct technical analysis and reporting	Cybersecurity Implementor	1	Priority 4
Develop and communicate, detailed and reasoned investigation reports	Penetration Tester	1	Priority 4
Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks	CISO	1	Priority 4
Follow and practice auditing frameworks, standards and methodologies	CISO	1	Priority 4
Guide and communicate with implementers and IT/OT personnel	Cybersecurity Implementor	1	Priority 4
Identify and exploit vulnerabilities	Cyber Threat Intelligence Specialist	1	Priority 4
Identify and exploit vulnerabilities	Cybersecurity Implementor	1	Priority 4
Identify and solve cybersecurity-related issues	Cybersecurity Architect	1	Priority 4
Identify needs in cybersecurity awareness, training and education	Cybersecurity Auditor	1	Priority 4
Identify threat actors TTPs and campaigns	Cyber Incident Responder	1	Priority 4
Identify, analyse and correlate cybersecurity events	Cyber Threat Intelligence Specialist	1	Priority 4
Influence an organisation's cybersecurity culture	Cybersecurity Architect	1	Priority 4
Integrate cybersecurity solutions to the organisation's infrastructure	CISO	1	Priority 4

Skills Areas	Role	New Skill	Priority
Integrate cybersecurity solutions to the organisation's infrastructure	Cybersecurity Architect	1	Priority 4
Integrate cybersecurity solutions to the organisation's infrastructure	Cybersecurity Researcher	1	Priority 4
Manage and analyse log files	Penetration Tester	1	Priority 4
Organise and work in a systematic and deterministic way based on evidence	Digital Forensics Investigator	1	Priority 4
Perform social engineering	Cyber Threat Intelligence Specialist	1	Priority 4
Practice all technical, functional and operational aspects of cybersecurity incident handling and response	Penetration Tester	1	Priority 4
Provide training towards cybersecurity and data protection professional certifications	CISO	1	Priority 4
Think creatively and outside the box	Cybersecurity Researcher	1	Priority 4
Think creatively and outside the box	Penetration Tester	1	Priority 4
Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies	Cybersecurity Auditor	1	Priority 4
Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies	Cybersecurity Architect	1	Priority 4
Use and apply CTI platforms and tools	Penetration Tester	1	Priority 4

Skills Areas	Role	New Skill	Priority
Work ethically and independently; not influenced and biased by internal or external actors	Cybersecurity Auditor	1	Priority 4
Stakeholder management	CISO	1	Priority 4
Change management	Cyber Threat Intelligence Specialist	1	Priority 4
Certifications	Cyber Threat Intelligence Specialist	1	Priority 4
Technical Proficiency	Cyber Threat Intelligence Specialist	1	Priority 4
Incident Response	Cyber Threat Intelligence Specialist	1	Priority 4
Continuous Learning	Cyber Threat Intelligence Specialist	1	Priority 4
Continuous Learning	Cyber Threat Intelligence Specialist	1	Priority 4
Assess the security and performance of solutions	Penetration Tester	1	Priority 3
Collaborate with other team members and colleagues	Cybersecurity Auditor	1	Priority 3
Communicate, coordinate and cooperate with internal and external stakeholders	Digital Forensics Investigator	1	Priority 3
Communicate, present and report to relevant stakeholders	Digital Forensics Investigator	1	Priority 3
Monitor new advancements in cybersecurity-related technologies	Digital Forensics Investigator	1	Priority 3
Work on operating systems, servers, clouds and relevant infrastructures	Digital Forensics Investigator	1	Priority 3
Anticipate cybersecurity threats, needs and upcoming challenges	Cybersecurity Researcher	1	Priority 2
Collect, evaluate, maintain and protect auditing information	Digital Forensics Investigator	1	Priority 2

Skills Areas	Role	New Skill	Priority
Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles	Cybersecurity Researcher	1	Priority 2
Develop and communicate, detailed and reasoned investigation reports	Cyber Threat Intelligence Specialist	1	Priority 2
Identify and solve cybersecurity-related issues	Cyber Threat Intelligence Specialist	1	Priority 2
Implement cybersecurity recommendations and best practices	Cybersecurity Researcher	1	Priority 2
Think creatively and outside the box	Cyber Threat Intelligence Specialist	1	Priority 2
Think creatively and outside the box	Cyber Incident Responder	1	Priority 2
Monitor new advancements in cybersecurity-related technologies	Cyber Threat Intelligence Specialist	1	Priority 1
Work under pressure	Digital Forensics Investigator	1	Priority 1

Legal Disclaimer
The European Commission's support to produce this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Project 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03


Digital4Security
Shaping Europe's cyber future
ADVANCED DIGITAL SKILLS
DIGITAL EUROPE PROGRAMME
Co-funded by
the European Union