D9.1

Cybersecurity skills framework

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D9.1 / V1.0
Work package contributing to the deliverable	WP9
Due date	January 2020 – M12
Actual submission date	31st January, 2020

Responsible organisation	L3CE
Editor	Edmundas Piesarskas
Dissemination level	PU
Revision	V1.0

Abstract	Initial Cybersecurity Skills Framework for SPARTA based on identified practices adapting them to EU and SPARTA approach.
Keywords	Skills management, Skills matrix, Skills framework

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Edmundas Piesarskas (L3CE)

Contributors (ordered according to beneficiary numbers)

Jan Hajný (BUT)

Olivier Levillain (IMT)

Sarunas Grigaliunas (KTU)

Egidija Versinskiene, Evaldas Bruze, Rimantas Zylius (L3CE)

Reviewers (ordered according to beneficiary numbers)

Daniel Keim (UKON)

Raimundas Matulevicius (UTARTU)

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

The proliferation of information and communication technologies is rapidly increasing, previously assumed "passive" devices become citizens of the Internet of Things. Industrial equipment, national and local infrastructures, automobiles are just a few important examples adding to the number of connected devices.

With the benefits and efficiencies gained by remote access and management of a variety of these devices, security risks increase at an even faster pace. As examples of cyber threats have already shown, well-designed attacks may have an impact on a national or even international scale, so securing connected devices, applications and infrastructure must go together with increased digitization and connectedness. Despite increased awareness and bold efforts, highly significant and consistently increasing shortages of cybersecurity professionals in the European Union and worldwide are well known, and these shortages continue to present major problems for public and private sectors alike. "Strategies for Building and Growing Strong Cybersecurity Teams" (ISC) CYBERSECURITY WORKFORCE STUDY 2019,[1] estimates, that there are 2.8 million cybersecurity professionals globally, while the gap is actually 4.07 million. The study notes that the current gap in Europe is 291,000, and this number has doubled since the year before.

Efforts to fill the skills gap requires EU, governments, academia, industry, as well as societies and professionals to take an active role. To undertake such concerted efforts, however, will require a common language which would allow for productive cybersecurity-related skills discussions across the Member States, industry, academia and professionals, so that actors can unambiguously understand each other.

The SPARTA project develops comprehensive threat intelligence models - advanced methodologies and technologies instrumental in identifying and fighting multilayer complex attacks. Cybersecurity skills necessary to comprehend complex current and emerging threats is one of the key principal building blocks.

So, SPARTA Work Package 9, Task 9.1. designates its efforts to analyse the state of knowledge on skills management, reviewing best practices and proposing the way forward with the development of an EU based cybersecurity skills framework. We have found that the JRC Cybersecurity domains taxonomy and the US-based National Initiative for Cybersecurity Education (NICE) are the most reasonable starting points for such an effort, providing a comprehensive and accommodative structure to incorporate the EU specific realities and emerging skills landscape.

Further, in the present document, the SPARTA Cybersecurity Skills Framework (SPARTA CSF) is proposed based on the structure of the NICE Framework, amended with EU specifics. The Framework is tested and validated for applicability, adaptability by industry and academia. Emerging threats are discussed with the further need to be incorporated into the Framework. SPARTA CS Framework 0.9 (for discussion purposes) is presented and described. Plans for further development of SPARTA CSF during the SPARTA Project are described, concluding with the Roadmap Workshop to decide on the applicability and future of the Framework.

A governance structure and key aspects of governance are outlined, open questions are formulated to kick start further discussion and establishment and management of the Framework.

Efforts presented in this documents should be considered as aiming to set in motion a process of development of a comprehensive European cybersecurity skills framework, that would provide a basis for continuous communication between different stakeholders (academia, industry, policymakers in EU and MSs, specialists, etc.) and would allow them to self-organize. There was no intent to produce a point-in-time snapshot of a skills matrix, which would rapidly lose its validity due to the fast pace of change of the cybersecurity field. This provision can be observed throughout the whole document and should be considered while using the material presented.

[1] https://www.isc2.org/Research/-/media/6573BE9062B64FC7B4B91F20ECC56299.ashx

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Purpose of the document

This document is put forward as an initial deliverable of the SPARTA project, Work Package 9 “Cybersecurity training and awareness” Task 9.1 “Cybersecurity Skills Framework Model Development”.

Here, we will review EU and non-EU efforts to classify skills in the area of cybersecurity and use such classification for analysis and guidance of academic curricula, industry needs and policymaking.

Best practices of current efforts will be identified and critically discussed.

Based on best practices, a consolidated approach will be proposed and an EU based skills matrix for cybersecurity is to be developed (SPARTA Cybersecurity Skills Framework).

We will further describe efforts to validate the developed SPARTA CS Framework.

We will also discuss acceptance and sustainability issues and will propose a governance structure that should ensure sustainability and continued relevance of the Framework.

The next steps necessary to develop the Framework further and attain public release will be taken up.

1.2 Approach used

The development of the SPARTA CS Framework is based on the assessment that there are currently several important initiatives, each of which aims to define a set of skills needed for securing organizations. However, these contain different levels of granularity and have been implemented with different levels of success.

In this document, we review initiatives in the field, select best practices and use these to develop the SPARTA CS Framework. We submit that this approach has significant advantages by allowing for:

- development of a comprehensive skills framework within a relatively short time frame (developing a framework of fine granularity and practical applicability would be an effort exceeding multiple years);
- re-use or re-purposing of existing knowledge, i.e. concepts and practices, which have already been tested in the field;
- an iterative approach that applies to learn and to test the new framework in practice, thereby making appropriate improvements quickly, in short cycles (as opposed to long cycles of academic thinking and overthinking concepts with very slow time to market);
- the new framework will borrow underlying concepts of, and maintain a natural bias towards, the “source” frameworks, and with strong governance and leadership, it will be transformed quickly into a full-fledged EU based framework, which will be firmly grounded on EU content.

Although this approach may have certain drawbacks, we strongly believe these can be mitigated in the following ways:

- adding anything new (concepts, categories, practices, etc.) to an existing framework may give rise to conflicting aspects that risk internal integrity: this will be mitigated by attracting top cybersecurity talent who will be responsible for adapting the framework to EU requirements both at the conceptual and detailed level without risking degradation of its integrity;

- the fast pace of technological change might impede successful deployment of the new framework, as it may not be able to adapt readily to the new landscape: however, a strong governance structure would ensure that modifications to the work-in-progress framework will be introduced in manageable portions, thus not risking its applicability in addressing the skills gap.

Taking into account the fact that the cybersecurity skills gap in the European Union continues to increase drastically, we contend that a common language across the Member States, academia, industry and policymakers is essential to filling this gap, hence our rationale for employing the results-oriented approach just described.

1.3 Implications for the SPARTA project

The SPARTA CS Framework, proposed in this document, will serve as a common denominator for the communication to the academia of the skills needed for a comprehensive cybersecurity approach that aims to develop or amend curricula to respond to the needs of emerging threats.

Thus, the SPARTA CS Framework will provide the necessary background for skills definitions in T-Shark and other technical work packages and will also be used in Work Package 9 Task 9.2 and Task 9.3 for the analysis of curricula, as well as for making appropriate adjustments.

1.4 Applicability beyond SPARTA project

We find that currently, EU lacks a comprehensive cybersecurity skills framework, which would allow policymakers to gather actionable data on the existing and emerging skills gaps. Overall, no agreed-upon framework allows for clear communication on cybersecurity skills outside of organizations – i.e. between different states, academia, or industry. Certification is one of the attempts in that direction, but certification alone cannot provide comprehensive and exhaustive coverage, it is not standardised across EU. Furthermore, the certification approach will always lack the ability to address the emerging skills dimension, which is one of the key areas addressed by SPARTA.

Although the SPARTA CS Framework is being developed within the context of the SPARTA project itself, nevertheless, from its very inception, it has aimed to be applicable to the EU as a whole. Here, we propose that the framework has the potential to become a common language for different actors to communicate, gather actionable information, and to act on it.

Chapter 2 Methodology

This chapter presents the path, which led to the results presented in this document.

Original design of task T9.1, responsible for deliverable D9.1 of the SPARTA Project, had the aim to point out the differences, survey the current status of knowledge, characterize the role of cybersecurity professionals, as well as other related roles regarding cybersecurity assurance and, based on these results, provide a consolidated cybersecurity skills framework throughout the EU by developing the Skills Matrix. Activities within this Task were also in close alignment with other activities within WP9 of the SPARTA project.

The methodological approach had to be changed during the initial phase of implementation. The original plan to survey the current status of knowledge and characterize different roles of cybersecurity professionals proved to be unattainable due to the complexity and limited possibilities of involving practitioners for the required in-depth interviews.

Further, methodology changes were motivated by the presence of various initiatives, aiming to analyse and structure the field of cybersecurity, including the definition of roles and knowledge required to secure systems and organizations. Since a variety of parallel activities are executed by some European organizations (e.g.: ENISA, ECSO, CEN, EGC, JRC, etc.), approaching them and sharing results of efforts of this work package in order to pool efforts for the development of a truly EU wide skills matrix seems most valuable. Integration efforts could help to develop and sustain high quality and a highly relevant taxonomy for the use of academia, industry and policymakers, and naturally, avoid possible overlapping efforts.

The guidelines of the new methodological approach are summarized further in this section.

2.1 Process of the development of SPARTA CS Framework

With the commencement of SPARTA Task 9.1, we consolidated a list of initiatives and documents to be reviewed, related to the field of cybersecurity skills, both within and outside of the European Union. This list was shared with all WP9 partners for feedback and we have included any missed and relevant initiatives (details provided in “Chapter 3. Analysis of existing initiatives relevant to the classification and management of cybersecurity skills”).

We analysed the documents and initiatives of EU organizations, specifically looking for input on what were the best efforts and approaches in structuring roles and corresponding knowledge/skills required to fulfil these roles in the field of cybersecurity. As well, we looked at what key challenges are encountered when applying these cybersecurity skills frameworks in the European Union. The extensive description and discussion of our review is provided in Chapter 3

Chapter 4 SPARTA Cybersecurity Skills Framework development describes the efforts to develop the actual framework resulting from the analysis of documents and various initiatives. Best practices are identified which provide insight into practical roles and skills classification with granularity fit for “real world”. Best practices then are amended to fill in the gaps identified in the analysis.

Chapter 5 is concerned with the validation efforts of the developed SPARTA CS Framework. Specifically, the Framework is tested to see if its capacities can be practically applied in the analysis and development of cybersecurity-related curricula, adaptability to emerging skills, and trends in emerging threats.

The results of framework development efforts are further described in Chapter 6 SPARTA Cybersecurity Skills Framework, where the backbone of the Framework version 0.9 is presented (version 0.9 is marked as “for discussion purposes only” and is still a work-in-progress). As well, an Interim governance structure including a panel of cybersecurity experts is proposed to complete the development of the SPARTA CSF Framework version 1.x (for SPARTA Project use, and further SPARTA CSF version 2.x for public use).

Chapter 6 also discusses issues of relevance and sustainability of the Framework, as well as putting forward open questions that should define the future of the Framework.

2.2 Relationship to other WP's and Tasks

The SPARTA CS Framework is an output of Task 9.1 and as such is a requirement as input to Task 9.2 in order to structure the analysis of cybersecurity programs in universities. The use of SPARTA CSF will continue throughout the project timeline.

T-Shark and other work packages of SPARTA, which develop concepts and technologies of comprehensive threat intelligence, will serve as inputs to the SPARTA CS Framework, specifically highlighting emerging threats and emerging skills which need to be addressed by the Framework. An effort to gather input from T-Shark for the purpose of testing adaptability is described in 5.4 Adaptability validation. Further cooperation with SPARTA T-Shark programme and other relevant work packages will continue until completion of the project.

Chapter 3 Analysis of existing initiatives relevant to classification and management of cybersecurity skills

In this section, we provide the results of our analysis of the current initiatives in the area of classification and management of cybersecurity roles and skills. For this purpose, we analysed relevant materials that have been developed by various entities (national, European Union and outside Europe). The further analysis focused on the identification of best practices, rather than an exhaustive listing of all documents in the area. Note that defence-related research is intentionally not included in the scope of the present document due to its specialised nature.

It is naturally assumed that a construct that aspires to be used as a comprehensive "Skills framework" must include at least the principal components such as roles and skills/knowledge, which should be defined and mapped accordingly, providing the full picture of the skills framework. This section examines various approaches of dealing with the skills gap in cybersecurity among professionals and non-practitioners alike with specific attention to answering the following questions:

- What are the major challenges in identifying roles and skills in the field of cybersecurity?
- Which Roles in cybersecurity should be covered in the skills framework?

How are the different components of skills/knowledge to be classified in the field of cybersecurity and how do these map to roles? The section includes an overview of the relevant documents, while others are not detailed, avoiding unnecessary information. The purpose of this review is not to criticise or challenge the works presented, but to focus on the evaluation of how the proposed taxonomies can be adapted to the SPARTA approach, how they address cybersecurity workforce management needs and how they can contribute to the development of the skills framework.

3.1 European initiatives

3.1.1 ENISA Report "Stock taking of information security training needs in critical sectors" December 2017

We first address the document by **ENISA,** Stock taking of information security training needs in critical sectors 2017. [2]

In the report, the threat landscape relevant to critical infrastructures is analysed and further analysis of training offerings are performed against it. The report gathers training needs in the areas of Energy, Transport, Drinking water supply and distribution[2], Banking and Financial market infrastructures, Health digital infrastructure and rates them against Training topics, namely:

- Communication (team exercises)
- Awareness Raising
- General Data Protection
- Vulnerability Assessment
- Identity & Access Management

[2] https://www.enisa.europa.eu/publications/stock-taking-of-information-security-training-needs-in-critical-sectors/at_download/fullReport

- Malware Analysis
- Network Analysis
- Web App Security
- Data Security
- Cloud Security
- Wireless Security
- Forensics Analysis
- Device & Endpoint Security
- ICS/SCADA Security
- Threat Intelligence
- Intrusion Prevention & Detection
- Incident Response Management
- Security of the Chain Supply
- Security of the Outsourcing
- Protection against APT
- Protection against DDoS attacks

While clearly having a face value and relevance to workforce management of critical infrastructures, such a classification scheme gathered from the professionals in the field does not aspire to be an exhaustive analysis of the cybersecurity field. Its relevance and validity are limited to the practice of securing critical infrastructures, their current threat landscape, and evaluating the current cybersecurity workforce situation. The ENISA report makes no claims about being a comprehensive overview of roles and skills in the cybersecurity field.

Overall, the ENISA report puts the notion of "threat" at the centre and views training programs as a mitigation strategy. Our search for "skills framework" starts off from a different vantage point, and aims to identify the roles and skills/knowledge required for securing the organization. Thus, ENISA input, while constituting a targeted practical approach for securing critical infrastructures, has little to contribute to modelling our skills framework.

3.1.2 ENISA cybersecurity education map

The ENISA project and corresponding website[3] visualizing and mapping curricula of universities in the field of cybersecurity deserve special mention.

The effort to collect, classify and map the curricula of universities in the Member States is a very important step which is targeted towards the development of a common language, shared information and actionable data. The ENISA database of curricula and mapping provides a level of visibility to policymakers, educators, industries and those looking for a career in cybersecurity.

Despite the fact that its reach is currently limited, this is a project of great relevance to SPARTA which aims to develop a comprehensive cybersecurity skills classification scheme. On the website, information is categorized only in relation to the Member States; while the category of "Discipline" is apparently self-created (they do not have fixed predefined classifier), so very similar subjects of two universities may easily fall under different Discipline category names.

In our estimation, ENISA could be advanced to the next level should the collected information be grounded in the recognized common skills categorization which would be aligned more explicitly with the various levels of educators, certifications, market data on-demand, etc. So, while currently being limited in its reach, the ENISA cybersecurity education map is truly a step forward in embracing the skills issue in the EU.

[3] https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities

3.1.3 ECSO "Position Paper: Gaps in European Cyber Education and Professional Training" 2018

ECSO's *Position Paper*[4] stresses the significance of the cybersecurity-related skills gap. Demand for cyber specialists and experts is greater than the supply and is increasing, the skills gap is visible in non-IT positions (lawyers, administrative personnel, healthcare professionals, service designers, and senior management...), and this gap is deemed likely to increase further. The *Paper* also notes that the cybersecurity field is considered to be a mainly "male profession", and due to this image problem, the cybersecurity field fails to attract female talent. The problem is further amplified by the lack of "cybersecurity knowledge of decision-makers".

The paper discusses the structural issues associated with the shortage of cybersecurity professionals:

- society and organisations are increasingly vulnerable;
- skills shortage, especially in universities, is dealt with by an "add-on" or short-term "patch" to the problem, neglecting the interdisciplinary nature of cybersecurity;
- professional training is usually focused on one specific skill and does not address the holistic nature of cybersecurity;
- cybersecurity is both a technical issue and a non-technical one, neither of these components can be overlooked;
- current educational curricula and training methodologies rarely provide proper access to real live data and networks to assess and learn from;
- degrees and certificates, on the one hand, are hard to compare, and professionals with similar credentials might still have different levels of competence; on the other hand, professional experience may not be recognised appropriately due to the lack of a degree or certificate.

The Position Paper goes on to suggest that cybersecurity should be viewed as an emerging meta-discipline, requiring not only technical knowledge. It should include a solid academic background, and a truly interdisciplinary understanding of the subject area, including a good understanding of the law, human factors/psychology, mathematics/cryptography, social sciences, economics, security & risk management/IT audit, as well as emphasizing academic values such as critical thinking. The value of university education lies in its holistic understanding of cybersecurity as a complex and multidisciplinary phenomenon, and in the ability to apply received knowledge and skills to solve real-life problems and development needs.

The Paper argues that academic education and professional training address different learning needs. Cyber education is a learning process focused on the synthesis of knowledge and skills, and the applicability of these skills for solving complex issues. Training, on the other hand, tends to be targeted at the acquisition of specific skill to a demonstrable level of competence. While certain specific cybersecurity skills can be obtained without a formal degree through professional training, certification of skills and knowledge should be addressed by professional organizations.

The *paper* concludes with proposals for "Solving the Dilemma of Cyber Security", namely that the demand for recognising the multidisciplinary nature of cybersecurity skills is increasing, while current education targets only certain spots in the large picture.

Among the proposals, "A cybersecurity educational framework shall be developed, aimed at delivering an integrated, multidisciplinary approach to cybersecurity training, exercising and certification, allowing different expertise in the organisation to understand how they shall cooperate to be prepared and defend the organisation. This integrated framework and methodology shall provide integration of academia and training industry know-how and the technical capabilities and

[4] https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf

resources available to deliver and validate the knowledge."[5] The importance of cooperation between academia, professional training and industry is strongly emphasised.

Although the *Position Paper* does not directly discuss the need for a cybersecurity skills framework, the theme of cooperation between various actors and its comprehensiveness, as well as the multidisciplinary nature of the cybersecurity field, is clearly at the visible core of the discussed document.

Being in alignment with this observation, the SPARTA response to these challenges is an effort to develop a cybersecurity skills classification, which could serve as a model for defining a field of cybersecurity, roles in the organization pertinent to the aim of securing the functioning of the organization, and skills necessary for executing these roles. Such classification could serve as a common denominator, a kind of common language allowing different actors – academia, professional training, industry, professionals and policymakers – to discuss cybersecurity skills development and collaborate both in the development of such a classification, and in the development and consumption of skills.

3.1.4 CEN European e-Competence Framework 3.0 2014

The European e-Competence Framework (e-CF) version 3.0 is a component of the European Union's strategy on 'e-Skills for the 21st Century.' It is designed as a tool to boost digital skills and the recognition of competencies and qualifications across countries and fosters ICT professionalism in Europe[6].

"The e-CF expresses ICT competence using the following definition: 'Competence is a demonstrated ability to apply knowledge, skills and attitudes for achieving observable results'. This is a holistic concept directly related to workplace activities and incorporating complex human behaviours expressed as embedded attitudes."[7]

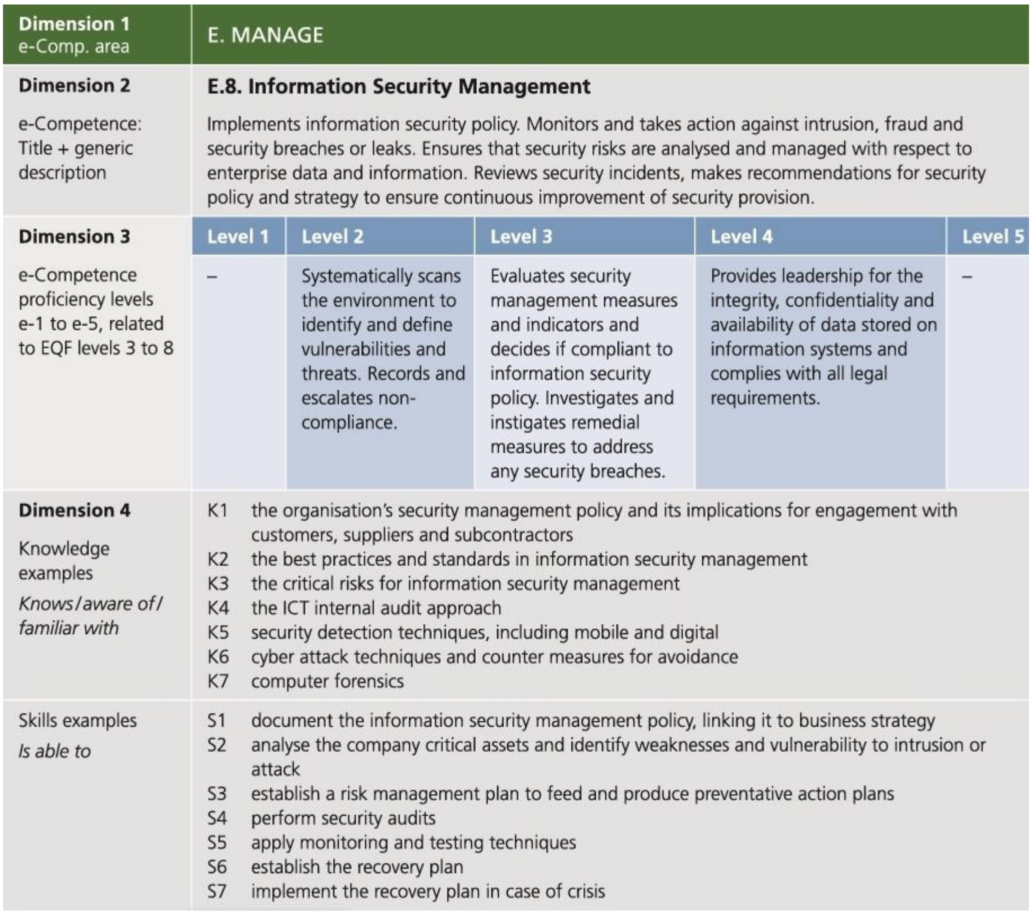
The e-CF provides a reference of 40 competencies as required and applied within the ICT workplace, using a common language for competencies (primarily knowledge and skills), and capability levels that can be understood across Europe.

The e-CF's structure consists of four dimensions:

- Dimension 1 includes 5 e-Competence areas: PLAN – BUILD – RUN – ENABLE – MANAGE (derived from standard ICT business processes);
- Dimension 2 consists of a set of reference e-Competencies for each area in Dimension 1, with 40 competencies identified in total;
- Dimension 3 provides descriptions for the proficiency levels of each of the e-Competencies – e-1 (Associate), e-2 (Professional), e-3 (Senior Professional/Manager), e-4 (Lead Professional/Senior Manager), e-5(Principal)), and these are associated with the European Qualifications Framework (EQF) levels 3 to 8.
- Dimension 4 contains a shortlist of knowledge and skills tied to the e-Competencies in Dimension 2.

For example, consider how these dimensions are employed in e-CF for the 'Information Security Management' category:

[5] "Gaps in European Cyber Education and Professional Training", Page 13, 2020.01.20 https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf
[6] www.ecompetences.eu
[7] "European e-Competence Framework 3.0", Page 5, 2020.01.20, http://www.ecompetences.eu/wp-content/uploads/2014/02/European-e-Competence-Framework-3.0_CEN_CWA_16234-1_2014.pdf



<table>
<tr><td><b>Dimension 1</b>
e-Comp. area</td><td colspan="5">E. MANAGE</td></tr>
<tr><td><b>Dimension 2</b>
e-Competence: Title + generic description</td><td colspan="5"><b>E.8. Information Security Management</b>
Implements information security policy. Monitors and takes action against intrusion, fraud and security breaches or leaks. Ensures that security risks are analysed and managed with respect to enterprise data and information. Reviews security incidents, makes recommendations for security policy and strategy to ensure continuous improvement of security provision.</td></tr>
<tr><td rowspan="2"><b>Dimension 3</b>
e-Competence proficiency levels e-1 to e-5, related to EQF levels 3 to 8</td><td><b>Level 1</b></td><td><b>Level 2</b></td><td><b>Level 3</b></td><td><b>Level 4</b></td><td><b>Level 5</b></td></tr>
<tr><td>–</td><td>Systematically scans the environment to identify and define vulnerabilities and threats. Records and escalates non-compliance.</td><td>Evaluates security management measures and indicators and decides if compliant to information security policy. Investigates and instigates remedial measures to address any security breaches.</td><td>Provides leadership for the integrity, confidentiality and availability of data stored on information systems and complies with all legal requirements.</td><td>–</td></tr>
<tr><td><b>Dimension 4</b>
Knowledge examples
<i>Knows/aware of/ familiar with</i></td><td colspan="5">K1 the organisation's security management policy and its implications for engagement with customers, suppliers and subcontractors
K2 the best practices and standards in information security management
K3 the critical risks for information security management
K4 the ICT internal audit approach
K5 security detection techniques, including mobile and digital
K6 cyber attack techniques and counter measures for avoidance
K7 computer forensics</td></tr>
<tr><td>Skills examples
<i>Is able to</i></td><td colspan="5">S1 document the information security management policy, linking it to business strategy
S2 analyse the company critical assets and identify weaknesses and vulnerability to intrusion or attack
S3 establish a risk management plan to feed and produce preventative action plans
S4 perform security audits
S5 apply monitoring and testing techniques
S6 establish the recovery plan
S7 implement the recovery plan in case of crisis</td></tr>
</table>

Figure 1: Information Security Management (*Source: http://ecompetences.eu)*

Dimension 2 “Title + Generic Description” has a strong relation to what would be considered as a Role definition in our Skills Classification model. While Dimension 4 relates strongly to the “skills/knowledge” category.

The focus on “Competence” allows the Framework to cover vast areas of ICT technologies providing some high-level structured insight into the capabilities of the person in his / her role. But this high-level approach lacks details when we turn our attention to the specific field of cybersecurity.

Although this Framework is able to serve some broader aims of structuring ICT field competencies, it lacks the depth, necessary to define comprehensive needs of entities in cybersecurity that entail analysing roles and defining the skills/knowledge elements, required to perform the role.

3.1.5 JRC European Cybersecurity Centres of Expertise Map. Definitions and Taxonomy

The Joint Research Centre[8] undertook an extensive analysis of existing cybersecurity domain research classifications and tried to merge these into a comprehensive classification scheme which would define the cybersecurity domain with respect to the EU landscape and would avoid redundancies of terms, definitions and domains.

JRC developed a taxonomy employing a three-dimensional matrix:

- Cybersecurity domains / Research domains
- Sectors/Industries
- Applications and technologies

[8] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf

The Cybersecurity Research Domains axis is focused on pure technological aspects of cybersecurity without specific application. The Applications and Technologies (e.g., Robotics, IoT, Mobile, etc.) vector specifies various ICT Technologies which require cybersecurity protection. Sectors (e.g., Energy, Transportation, Healthcare, etc.) are different industries in which cybersecurity technologies are applied and which face sector-specific challenges.

Cybersecurity Technologies include the following categories:

- Assurance, Audit, and Certification;
- Cryptology (Cryptography and Cryptanalysis);
- Data Security and Privacy;
- Education and Training;
- Operational Incident Handling and Digital Forensics;
- Human Aspects;
- Identity and Access Management;
- Security Management and Governance;
- Network and Distributed Systems;
- Software and Hardware Security Engineering;
- Security Measurements;
- Legal Aspects;
- Theoretical Foundations;
- Trust Management, Assurance, and Accountability.

The Applications and Technologies vector contains the following categories:

- Artificial intelligence;
- Big Data;
- Blockchain and Distributed Ledger Technology (DLT);
- Cloud and Virtualisation;
- Embedded Systems;
- Hardware technology (RFID, chips, sensors, routers, etc.)
- Industrial Control Systems (e.g. SCADA);
- Information Systems;
- Internet of Things;
- Mobile Devices;
- Operating Systems
- Pervasive systems
- Quantum Technologies
- Robotics;
- Satellite systems and applications;
- Supply Chain;
- Vehicular systems

The following Sectors are considered by JRC:

- Audio-visual and media
- Defence
- Digital Infrastructure
- Energy
- Financial
- Government and public authorities
- Health
- Maritime
- Nuclear
- Public safety
- Tourism

- Transportation
- Smart ecosystems
- Space
- Supply Chain

Visual representation of the matrix is provided in the figure below:

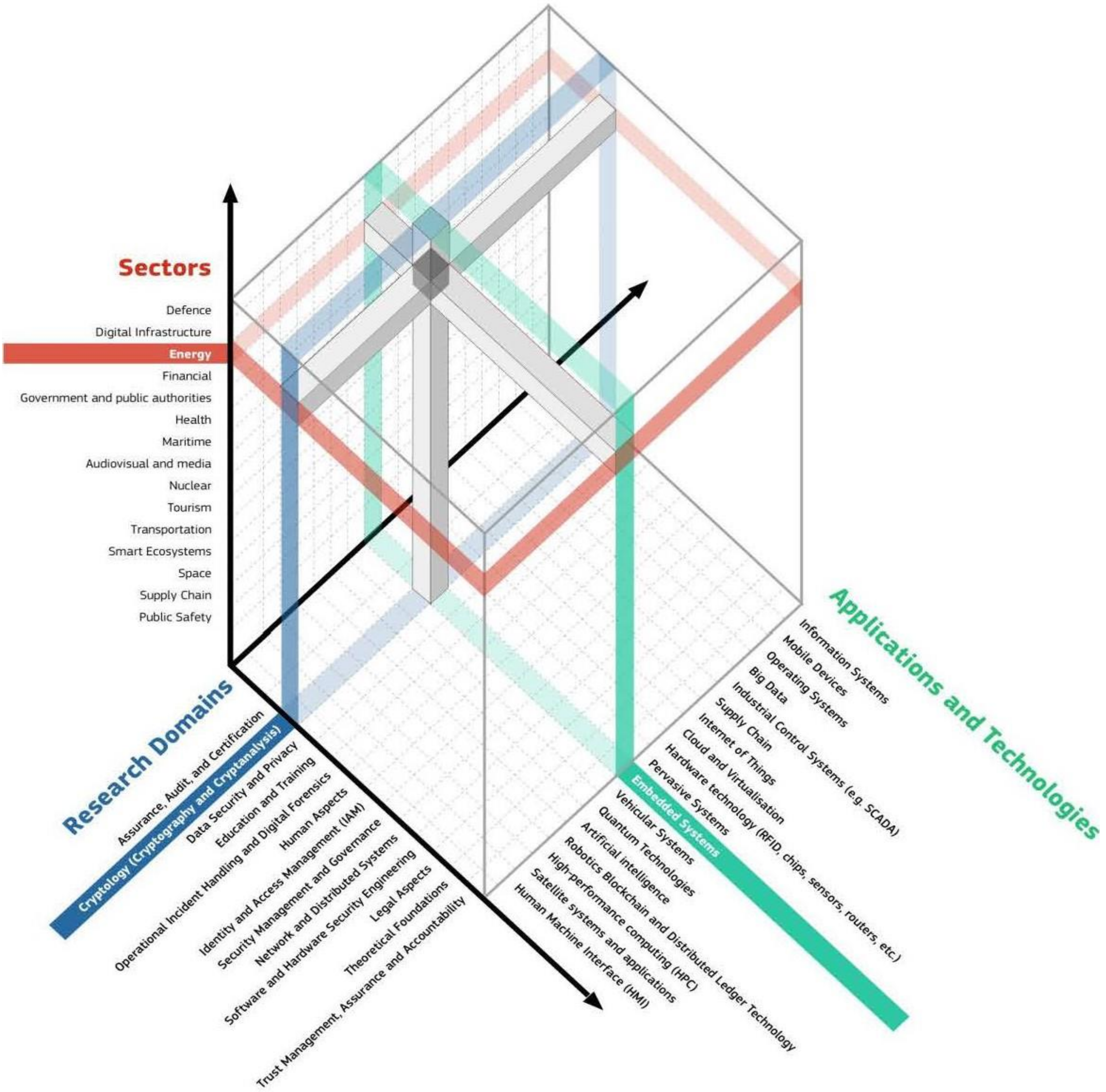

Sectors
Defence
Digital Infrastructure
Energy
Financial
Government and public authorities
Health
Maritime
Audiovisual and media
Nuclear
Tourism
Transportation
Smart Ecosystems
Space
Supply Chain
Public Safety
Research Domains
Assurance, Audit, and Certification
Cryptology (Cryptography and Cryptanalysis)
Data Security and Privacy
Education and Training
Operational Incident Handling and Digital Forensics
Human Aspects
Identity and Access Management (IAM)
Security Management and Governance
Network and Distributed Systems
Software and Hardware Security Engineering
Legal Aspects
Theoretical Foundations
Trust Management, Assurance and Accountability
Applications and Technologies
Information Systems
Mobile Devices
Operating Systems
Big Data
Industrial Control Systems (e.g. SCADA)
Supply Chain
Internet of Things
Cloud and Virtualisation
Hardware technology (RFID, chips, sensors, routers, etc.)
Pervasive Systems
Embedded Systems
Vehicular Systems
Quantum Technologies
Artificial intelligence
Robotics Blockchain and Distributed Ledger Technology
High-performance computing (HPC)
Satellite systems and applications
Human Machine Interface (HMI)

Figure 2: JRC Matrix (*Source: https://publications.jrc.ec.europa.eu)*

"Sectors" and "Research Domains" are further subdivided into subdomains, whereas Applications and Technologies do not have their sub-categories listed.

This taxonomy aspires to classify and provide a common dictionary for further practice and research in the cybersecurity field.

The defined taxonomy is recognized by SPARTA and EU multiple stakeholders as a benchmark framework. As described in the initial document of the SPARTA project "D3.1: Initial SPARTA SRIA Roadmap v0.1": JRC's set of Cybersecurity Technologies appears to be comprehensive, i.e., covers all aspects of cybersecurity; while Applications and Technologies, and Sectors, domains contain the most evident and essential categories, these can hardly be considered as a complete list (additional elements can be added if needed).

The JRC taxonomy paper itself notes that its approach is not fully exhaustive, nor does it represent a comprehensive model, but is subject to evolving structures and modification. The JRC paper states in conclusion that "The resulting three-dimensional taxonomy presented in Section 3 is not static, but it is open to modifications and must be understood as a living semantic structure which will change during the years to keep the pace of the fast evolution of the digital world."[9]

Although the JRC taxonomy analyses the application of cybersecurity in a wider context by expanding on the non-technological and human factors, it should be noted that the JRC framework does not have a strong focus on skills per se. As the first step of this ambitious initiative, it focuses on a clear definition of the cybersecurity context, its domains of application, research and knowledge, rather than a cyber-workforce oriented framework that covers all the work-related roles and skills.

Thus, it can be concluded that the JRC taxonomy is very important as a classifier of the cybersecurity field within the EU landscape, however, it does not fully satisfy the needs of cyber workforce development.

It is important to mention that the cybersecurity field is developing extremely rapidly and such frameworks risk losing their relevance very quickly if these are not regularly updated through authoritative processes. Therefore, any work based on the JRC taxonomy should carefully study sources and methodology and provide input for further development of the taxonomy model.

Other frameworks specific to skills must be used or developed for this purpose.

3.1.6 UK - Initial National Cyber Security Skills Strategy

The UK's Initial National Cyber Security Skills Strategy[10] published in December 2018, reiterates the huge supply gap of cybersecurity skills in the market and the fact that it continues to increase. According to the Strategy document, this naturally might be attributed to its being a young profession: "While there has been significant progress to develop the cybersecurity profession in the UK, more needs to be done. The taxonomy around cybersecurity can be confusing and routes into and through cybersecurity careers can be hard to navigate." To deal with this issue, the UK government has set itself the goal of bringing out The Cyber Security Body of Knowledge (CyBOK)[11] defining the field of cybersecurity. The first version was published in October 2019.

It is important to note that CyBOK does not address skills and roles challenges, but rather defines 19 Knowledge Areas into a coherent framework. However, the strategy is clearly aware of the need to align its 'body of knowledge' with the structures of the requirements of the workforce, and notes: "...in the US the National Institute of Standards and Technology (NIST) is leading the National Initiative for Cyber Security Education (NICE) which is focused on cybersecurity education, training and workforce development. Part of the work to deliver on this strategy will be to explore further how the outputs of the various initiatives align with the UK led CyBOK work."

[9] "European Cybersecurity Centres of Expertise Map" ,Page 36, 2020.01.20 https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf

[10] https://www.gov.uk/government/publications/cyber-security-skills-strategy

[11] https://www.cybok.org/media/downloads/CyBOK_version_1.0_YMKBy7a.pdf

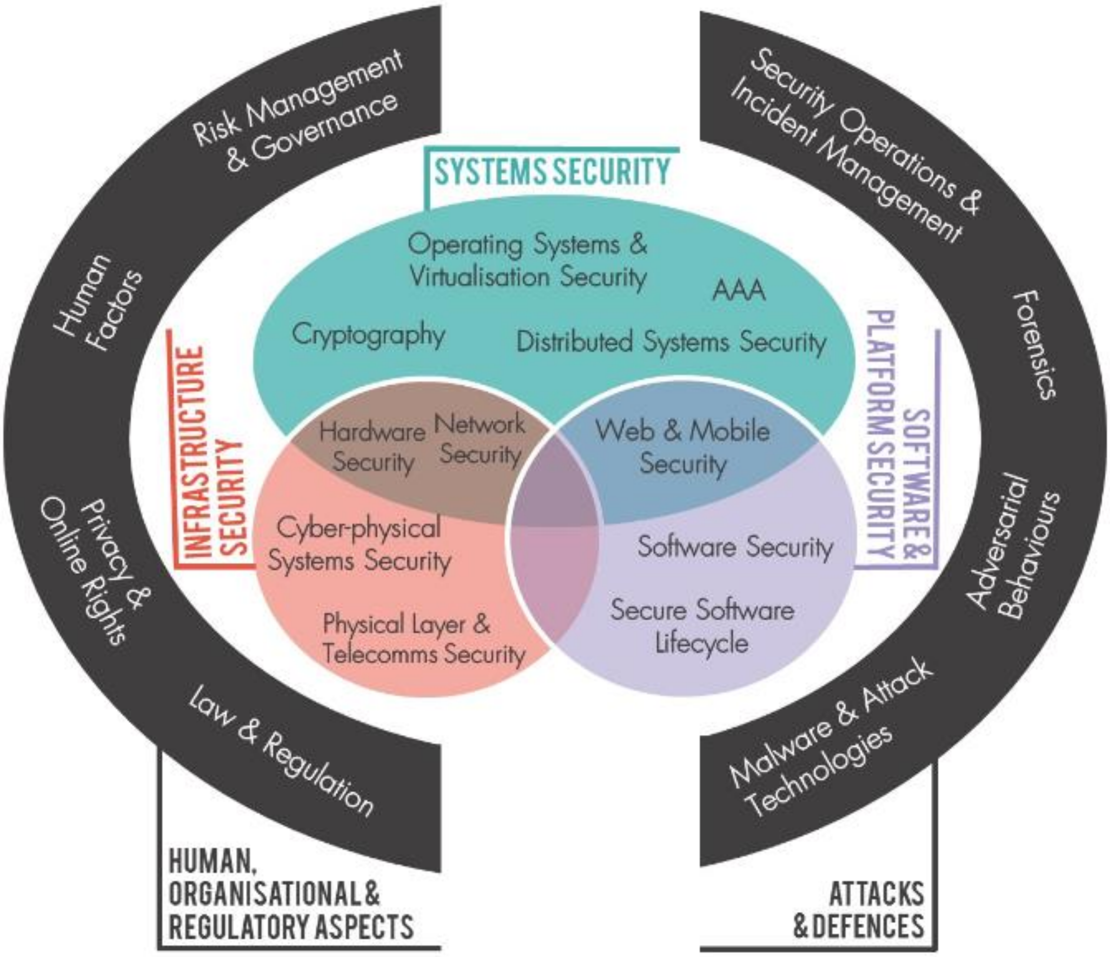

Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
AAA
Cryptography
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Web & Mobile Security
Cyber-physical Systems Security
Physical Layer & Telecomms Security
Software Security
Secure Software Lifecycle
SOFTWARE & PLATFORM SECURITY
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

Figure 3: The 19 Knowledge Areas (KAs) in the CyBOK Scope *(Source: https://www.cybok.org/)*

CyBOK systematizes knowledge which is needed in order to secure an organization and its assets. But it does not define specific roles in the organization, or what specific knowledge roles should have. Without a doubt, CyBOK advances clarity of the cybersecurity field and systematizes knowledge, thereby helping the cybersecurity profession, but it does not directly address the definitions of roles and knowledge categories.

3.2 Non-EU initiatives

3.2.1 National Initiative for Cybersecurity Education (NICE)

In the present analysis, we have identified the NICE Framework as a comprehensive and highly practical model that takes into account an exhaustive list of tasks that have to be performed in the fields of cybersecurity in various organizations. These tasks are associated with certain roles, and correspondingly, what knowledge - skills - abilities a role should have in order to be able to perform its assigned tasks. In this way, the framework models comprehensively the key tasks - roles - knowledge - skills - abilities in the cybersecurity field. However, the framework does not analyse processes of organizational hierarchies and thus can be very easily adapted to the realities of a particular organization.

This framework may seem overwhelming but has proven to be highly practical and applicable for day to day workforce management and planning. The formal categorization of the framework follows:

> The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework - NIST Special Publication 800-181), National Institute of Standards and Technology, U.S. Department of Commerce, August 2017.[12]
>
> An integrated cybersecurity workforce capable of meeting the needs of an organization requires a staff of knowledgeable and experienced people including technical and non-technical personnel with the capability of designing, developing, implementing, and maintaining defensive and offensive cyber strategies to counter threats that exploit vulnerabilities in growing and evolving cyberinfrastructures and to protect the nation from existing and emerging cybersecurity challenges.

NICE is a partnership between government, academia, and the private sector working together for the purpose of keeping America secure. The Framework serves as:

- a reference structure that categorizes and describes the interdisciplinary nature of cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity strategies implemented by an organization;
- a guide to identifying, recruiting, developing, and retaining cybersecurity talent;
- a reference source on different aspects of cybersecurity workforce development, planning, training, and education.

Framework objectives

- to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development;
- to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals;
- to cultivate an integrated cybersecurity workforce that is globally competitive from hire to retire;
- to promote nationwide initiatives that increase the number of people with the knowledge, skills, and abilities to perform the tasks required for cybersecurity work.

Components of the NICE Framework

There are **7 categories** that provide the overarching organizational structure of the Framework. Each **category** is composed of **33 Specialty Areas** and each one represents an aspect of concentrated work, or function, within cybersecurity.

52 Work Roles are the most detailed groupings of cybersecurity and related work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role.

"Knowledge, Skills, and Abilities (KSAs) are the attributes required to perform work roles and are generally **Knowledge, Skills, and Abilities (KSAs)** are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training".[13]

Tasks are specifically defined pieces of work that, combined with other identified **Tasks**, compose the work in a specific speciality area or work role.

The NICE Framework components describe cybersecurity work. As discussed, each Category is composed of Specialty Areas, each of which is composed of one or more work roles. Each work role,

[12] https://doi.org/10.6028/NIST.SP.800-181

[13] "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework", Page 5, 2020.01.20, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

in turn, includes KSAs and Tasks. The figure below depicts the structure of these hierarchical relationships.

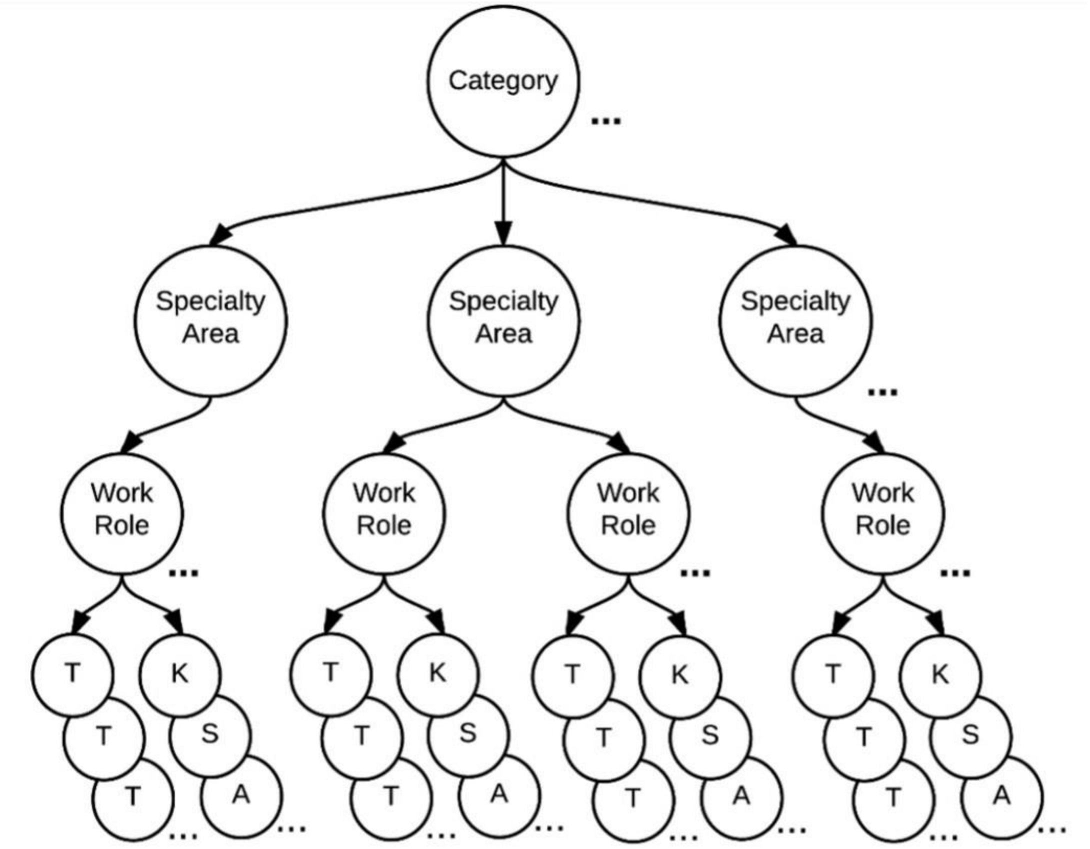


Figure 4: Structure and hierarchical relationships of NICE Framework *(Source: "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework", Page 6, 2020.01.09 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf(*

Each of these components is defined precisely in the NICE document in tabular format. As an example, consider the table below for the 7 Categories.

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Table 1: Categories of roles in the NICE Framework (Source: https://doi.org/10.6028/NIST.SP.800-181)

Indeed, it is our contention that the NICE Framework provides the best example of the distinguishing characteristics necessary to allow for a viable use of the Role category in dealing with strategic issues related to cybersecurity Skills development. More specifically, a Skill in NICE is an observable *competence* to perform a learned psychomotor act, and this means having the ability or *competence* in applying tools, architecting frameworks, or analysing processes in order to achieve beneficial results in the ICT domain generally or, in our case, specifically in the cybersecurity domain.

Significantly, in NICE, the relevance and importance of the Work Role category is clearly evident because KSAs and Tasks are associated explicitly with Work Roles. The following passage from NICE should make this evident:

> Work Roles are the most detailed groupings of cybersecurity and related work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role. Work is performed in a job or position is described by selecting one or more work roles from the NICE Framework relevant to that job or position, in support of mission or business processes.

To illustrate the level of detail here we provide only a glimpse of the list of tasks and KSAs.

Example list of tasks (overall there are 1007 tasks attributable to roles):

Task	Task Description
T0001	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.
T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.
T0006	Advocate organization's official position in legal and legislative proceedings.
T0007	Analyze and define data requirements and specifications.
T0008	Analyze and plan for anticipated changes in data capacity requirements.
T0009	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.
T0010	Analyze organization's cyber defence policies and configurations and evaluate compliance with regulations and organizational directives.
T0011	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.
T0012	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.
T0013	Apply coding and testing standards, apply security testing tools including "fuzzing" static- analysis code scanning tools, and conduct code reviews.
T0014	Apply secure code documentation.
T0015	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.
T0016	Apply security policies to meet security objectives of the system.

Table 2: Example list of NICE Framework tasks (Source: https://doi.org/10.6028/NIST.SP.800-181)

Example list of knowledge items (overall 630 knowledge items are identified):

KSA	Description
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.

KSA	Description
K0002	Knowledge of risk management processes (e.g., methods for assessing and
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004	Knowledge of cybersecurity and privacy principles.
K0005	Knowledge of cyber threats and vulnerabilities.
K0006	Knowledge of specific operational impacts of cybersecurity lapses.
K0007	Knowledge of authentication, authorization, and access control methods.
K0008	Knowledge of applicable business processes and operations of customer
K0009	Knowledge of application vulnerabilities.
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.

Table 3: Example list of NICE Framework knowledge items (Source: https://doi.org/10.6028/NIST.SP.800-181)

Example list of skills (overall there are 374 skills identified):

Skill	Description
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security
S0002	Skill in allocating storage capacity in the design of data management systems.
S0003	Skill of identifying, capturing, containing, and reporting malware.
S0004	Skill in analysing network traffic capacity and performance characteristics.
S0005	Skill in applying and incorporating information technologies into proposed solutions.
S0006	Skill in applying confidentiality, integrity, and availability principles.
S0007	Skill in applying host/network access controls (e.g., access control list).
S0008	Skill in applying organization-specific systems analysis principles and techniques.
S0009	Skill in assessing the robustness of security systems and designs.
S0010	Skill in conducting capabilities and requirements analysis.

Table 4: Example list of NICE Framework skills (Source: https://doi.org/10.6028/NIST.SP.800-181)

Example list of abilities (overall 176 abilities are identified):

Ability ID	Description
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
A0002	Ability to match the appropriate knowledge repository technology for a given application or environment.
A0003	Ability to determine the validity of technology trend data.
A0004	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.
A0005	Ability to decrypt digital data collections.
A0006	Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures.
A0007	Ability to tailor code analysis for application-specific concerns.
A0008	Ability to apply the methods, standards, and approaches for describing, analysing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defence Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).
A0009	Ability to apply supply chain risk management standards.
A0010	Ability to analyze malware.

Table 5: Example list of NICE Framework abilities (Source: https://doi.org/10.6028/NIST.SP.800-181)

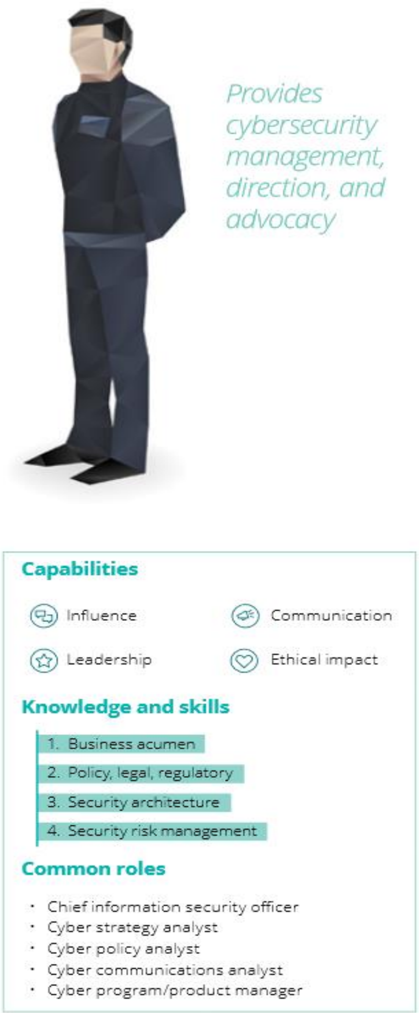
Lastly, NICE provides a listing of cybersecurity Skills, which reflect the observable *competence* necessary to perform a learned psychomotor act, and the descriptions of the Skills contained in this list have a direct relation to each Work Role defined in NICE. Moreover, the listing of cybersecurity Abilities assumes that an Ability is a *competence* to perform an observable behaviour, or a behaviour that results in an observable product, and this also implies that there is a direct connection to each work Role.

Our analysis has revealed that criticism of the NICE Framework is valid in so far as it is unable to meet the needs of SPARTA; nor can it serve as a skills framework for the wider EU context.

- NICE has been developed on US standards, refers to US federal legislation and regulations and clearly lacks European Union specific features.
- Some authors point out that NICE lacks the definition of skills/knowledge levels (although certain knowledge may be attributed to a role, NICE does not define the level of specific knowledge required, e.g. introductory, intermediate or expert).

- Since NICE is very much focused on the current realities of the cybersecurity field, its capacity to include emerging threats, emerging roles and emerging skills/knowledge levels is still to be determined.
- We encountered criticism that the level of detail of the NICE Framework is overwhelming to some of the practitioners, rendering it unusable. Still, we found this position to be extreme, as most feedback was very positive about the high level of detail that the framework demonstrates, and its powerful potential due to this aspect.

In summary, the NICE Framework is a flexible, open-ended resource that will strengthen an organization's ability to communicate consistently and clearly about cybersecurity work and its cybersecurity workforce. It allows organizations to develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.



Capabilities

Influence
Communication
Leadership
Ethical impact

Knowledge and skills

1. Business acumen
2. Policy, legal, regulatory
3. Security architecture
4. Security risk management

Common roles

- Chief information security officer
- Cyber strategy analyst
- Cyber policy analyst
- Cyber communications analyst
- Cyber program/product manager

Figure 5: Illustration of Deloitte role description *(Source: https://www2.deloitte.com)*

3.2.2 Study “The changing faces of cybersecurity Closing the cyber risk gap”

The study undertaken by Deloitte Canada Consulting Group & Toronto Financial Services Alliance[14] builds on The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework - NIST Special Publication 800-181), National Institute of Standards and Technology, U.S. Department of Commerce, August 2017.

Deloitte’s focus is cyber risk gaps with special attention to future technology trends and issues, specifically on cyber risk in a data-driven distributed, machine-enabled world.

The Deloitte study goes on to suggest that although positive progress in business, academia, and government has been made, nevertheless, current efforts are likely not sufficient to address the cyber talent shortage effectively. As some have argued, throwing more technology at the problem is not a panacea. What is needed, is a fresh perspective, specifically a new cyber talent framework that can inspire new and innovative ways to tackle the problem by viewing it through a human-centric lens.

To be effective, the study argues, such a framework needs to be stable and informative, featuring stable groupings of talent (focused on enduring capabilities over ephemeral skills), and providing a useful reference point to understand and plan for changing talent requirements in the context of evolving technology. It also needs to be understandable for non-security individuals, making the cybersecurity profession more accessible and inclusive for a broader audience.

The study defines seven “personas” – types of personalities, the personification of the set of capabilities, some sort of psychological inclination, that apply to various cybersecurity functions.

List of personas:

- Strategist - Provides cybersecurity management, direction, and advocacy;
- Advisor - Advises on the concept, design, and/or building of secure systems and networks;
- Defender - Supports, administers, and maintains the security of systems, data, and networks;
- Firefighter - Identifies, analyzes, and mitigates threats to internal systems, data, and networks;
- Hacker - Conducts specialized threat detection and deception activities to identify and mitigate cybersecurity risks;
- Scientist - Performs specialized analysis of threat intelligence, and cryptographic and security information to improve security posture;
- Sleuth - Investigates cybersecurity events or crimes related to systems, networks, and digital evidence.

Personas are defined by capabilities, knowledge and skills and mapped to NICE work roles.

This study demonstrates an interesting effort to humanize the cybersecurity profession, or rather to provide insight that the cybersecurity profession is in need of very different types of personalities and sets of skills. While this proposition does not provide straightforward input to the development of skill classification, it should be considered as a promising tool for career path planning, talent recruitment and professional orientation, and might provide an additional, “soft” dimension. Once more it highlights the very human nature of the cybersecurity profession, and that personality traits play a very important role in this context.

On the other hand, this study shows how various practical applications relevant to different stakeholders can be built on a robust skills framework, thereby enhancing accessibility to the cybersecurity profession from different angles.

[14] https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

3.2.3 New Brunswick Adopts the NICE Framework

In Canada, a leadership role in cyber skills development has been taken up by one of the smallest of 10 provinces, namely, New Brunswick.

The government of New Brunswick launched CyberNB in May 2016 to position the province as a cybersecurity epicentre in Canada. As a Special Operating Agency of the government, CyberNB's mandate is to accelerate the cybersecurity sector's pace of growth to secure the associated economic benefits and to ensure the public has access to a safe and resilient internet.

Access to highly skilled talent is widely recognized as a major driver of the cybersecurity sector where specialized skills, certifications, and security clearances are integral to ensuring the workforce is capable and secure. A key pillar of the CyberNB strategy was the establishment of a talent pipeline to support both the existing cybersecurity companies and to attract new businesses and investment. In 2017, CyberSmart, a key component of CyberNB, was initiated as a comprehensive workforce development strategy targeting youth development, workforce standards, training and recruitment, and career awareness.

The CyberSmart team quickly took into account that in Canada the growth in digital jobs had outpaced the overall economy at the time by over four to one over a two-year period, leading to strong demand for 182,000 skilled IT workers by 2019. This led to the identification of the NICE Framework and its leadership as potential collaborators to address the need for a comprehensive cybersecurity workforce development framework to guide New Brunswick's education, training, and recruitment programs and activities. Bilateral meetings ensued between NICE representatives and CyberNB, as well as a number of New Brunswick industry leaders.[15] The CyberSmart team were particularly impressed by the comprehensive nature of the NICE Framework, along with the high degree of acceptance in the United States cybersecurity sector, as well as other parts of the globe such as Australia, and elsewhere.

The Cybersecurity Workforce Development Initiative (CWDI) was established in February 2018 by CyberNB and CyberSmart with the aims of promoting the use of the NICE Framework within the New Brunswick cybersecurity ecosystem; ensuring alignment between cybersecurity certifications and the NICE standards and framework; and collecting, analysing, and disseminating cybersecurity workforce data.

It was agreed that the adoption of the NICE standards and framework offered New Brunswick the following specific benefits:

1. Provided New Brunswick with a state-of-the-art cybersecurity skills and workforce development framework to guide education, training and recruitment programs and activities;
2. Would avoid considerable development costs in duplicating a similar framework for New Brunswick; and
3. Promoted cross-border alignment in cybersecurity skills and workforce development.

The cross-border aspect was particularly important as transmission of electricity between the province and the US was a specific example of a shared interest in critical infrastructure. Moreover, a common cybersecurity lexicon and skills development framework would ensure alignment of cybersecurity expertise and expedite inter-jurisdictional communication and teamwork in all areas of bilateral cybersecurity interaction. Addressing multi-country cybersecurity attacks from individuals, criminal organizations or foreign states would also be expedited if the United States and Canada shared common talent development standards.

Presently, CyberNB is working with the national partners of NICE in advocating the adoption of the NICE Framework in the rest of Canada.

This is a good example, illustrating the possibilities and benefits of adopting and using already developed solutions.

[15] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-spring-2018-enewsletter

3.2.4 *Cyberseek.org project*

This is a project[16] supported by NICE and developed by several market players. It connects actual market data in the US and maps it with the NICE Framework as a result of providing a highly practical, impactful visual tool for career planning for individuals, for educators, and companies.

The project connects actual market data about:

- Job openings in the cybersecurity field in the US, for particular positions, skills, and geography;
- Filled positions;
- The average salary for the position;
- Top skills requested, top certifications requested;
- Mapping to work role in the NICE Framework;
- Tools for planning career in the cybersecurity field;
- Etc.

This project is a very powerful demonstration brought about by mapping of real-world market data in a meaningful context and representing it in a concise and visual manner, relevant to the user.

The figure below illustrates an interactive map of the planning of entry and advancement in the cybersecurity field. A user can explore how roles are connected from the perspective of seniority and what roles can be developed from the current viewer's position.

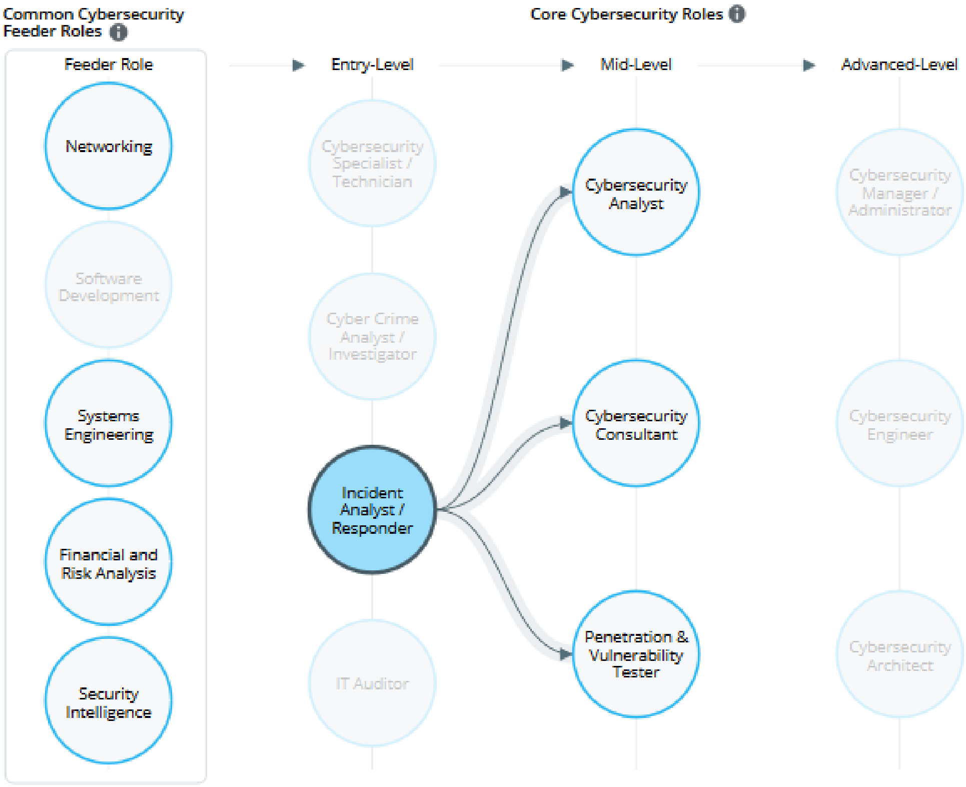
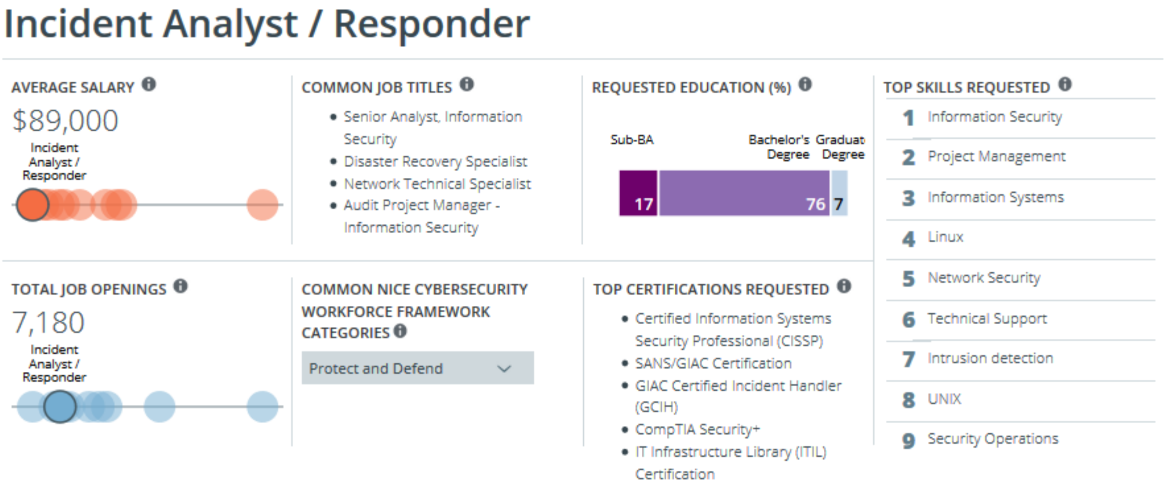


Figure 6: Interactive map illustration *(Source:* https://www.cyberseek.org/pathway.html)

[16] https://www.cyberseek.org/

In addition, a user can view features of the work role of interest and its different aspects – evaluate demand and supply, geographical specifics, average salary, top skills etc. Consider the following details:



Incident Analyst / Responder

AVERAGE SALARY

$89,000

Incident Analyst / Responder

COMMON JOB TITLES

- Senior Analyst, Information Security
- Disaster Recovery Specialist
- Network Technical Specialist
- Audit Project Manager - Information Security

REQUESTED EDUCATION (%)

Sub-BA	Bachelor's Degree	Graduat Degree
17	76	7

TOP SKILLS REQUESTED

1 Information Security
2 Project Management
3 Information Systems
4 Linux
5 Network Security
6 Technical Support
7 Intrusion detection
8 UNIX
9 Security Operations

TOTAL JOB OPENINGS

7,180

Incident Analyst / Responder

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

Protect and Defend

TOP CERTIFICATIONS REQUESTED

- Certified Information Systems Security Professional (CISSP)
- SANS/GIAC Certification
- GIAC Certified Incident Handler (GCIH)
- CompTIA Security+
- IT Infrastructure Library (ITIL) Certification

Figure 7: Features of the work role (*Source:* https://www.cyberseek.org/pathway.html)

The Cyberseek.org project demonstrates to us that a practical skills framework can be used in a variety of ways, and by integrating with market data can be leveraged as a tool to provide relevant and actionable information to individuals and organizations in the field.

The NICE Framework, in this example, proves to be a highly powerful tool in the US, which allows self-organization of various stakeholders which in their individual ways act and contribute to the augmentation and development of the cybersecurity workforce.

3.3 Roles and Skills in the field of cybersecurity

Analysis of documents related to the identification of the skills gap in the field of cybersecurity has reinforced the notion that no single classification of skills is used in the EU, and that industry demands, academic curricula, and professional training programs in relation to cyber skills are patchy. In any case, market forces ensure that only the most acute challenges of industries are being addressed.

As the cybersecurity field receives its fair share of attention, threat analysis, profiles, strategies and instruments of addressing these are developed into more or less comprehensive frameworks (cybersecurity body of knowledge being just one example). But there remains an unaddressed gap between what needs to be done to secure the organization and who specifically in the organization possesses the skills and knowledge necessary to deal with ominous threats. Only the NICE Framework, developed and sustained in the US, was referred to in multiple source documents in our analysis.

Further, we discuss the view of cybersecurity through the lens of workforce development, thus bringing roles and the skills/knowledge view into discussion.

3.3.1 Analysis of the definition of roles

In developing the skills framework exhaustive classification of roles, functions, and actual tasks, work scope performed in daily activities is of critical importance. Definition of roles usually is a starting point, providing the complete scope of “what are specialists doing in the organization, unit or role”. Only by understanding activities, described by tasks, can one acquire a full understanding of the skills needed to perform those tasks.

The European documents that we analysed did not describe roles in full, only partially. For example, The European e-Competence Framework (e-CF) version 3.0 document provides the scope of functions derived from standard ICT business processes. We found this to be the only EU description that can be used for the development of a skills matrix, as the approach followed includes roles – tasks – knowledge, even though it has some limitations: (i) cybersecurity is just one of the components within e-CF framework which is based on standard business processes; and (ii) it functions on a highly abstract level, not allowing for detailed descriptions of functions performed within the domain.

The best example of conceptualization of activities within the scope of cybersecurity and defining Roles is the NICE Framework (discussed in the documentary review.). The NICE Framework provides detailed and exhaustive descriptions, aiming to capture all roles involved in the process of securing an organization. It is worth noting, that a comprehensive skills framework must aim to achieve exhaustive surface coverage. Users of such a framework should then be able to select relevant roles that apply to their specific organization.

To summarise, the NICE structure and definition of Roles was determined to be the only close fit for our purposes and suitable for further skills framework development.

3.3.2 *Analysis of the definition of skills*

Skills are partly covered in the e-CF framework, though their true focus is a higher level "competence" notion.

Cyber Security Skills in the UK Labour Market[17] provide very inclusive, but rather general definitions, which are related more to an organization, rather than to a person. Consider the following passage:

> "We define cyber security skills as the combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complimentary soft skills that allow organisations to:
>
> - understand the current and potential future cyber risks they face
> - create and effectively spread awareness of cyber risks, good practice, and the rules or policies to be followed, upwards and downwards across the organisation
> - implement the technical controls and carry out the technical tasks required to protect the organisation, based on an accurate understanding of the level of threat they face
> - meet the organisation's obligations with regards to cyber security, such as legal obligations around data protection
> - investigate and respond effectively to current and potential future cyber-attacks, in line with the requirements of the organisation
>
> This defines the core set of knowledge and skills that organisations need to either have within their workforce or seek externally (for example, if they outsource their cyber security or take on external consultants). Those working in the wider cyber security industry – developing cyber security products or services, or carrying out fundamental research – may require additional skills, such as the technical expertise and skills needed to research and develop new technologies, products or services."

This notion of skill is not operationalized in further documents related to workforce development, and its applicability for real-world workforce development is yet to be seen.

The NICE Framework, on the other hand, operationalizes theoretical concepts into practice. It defines Works Roles and corresponding Tasks, which these roles are entrusted to perform, as well

[17] https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market

as Knowledge, Skills and Abilities (KSAs) which are needed for specific roles to perform attributed tasks.

According to NICE:

- ***Knowledge, Skills, and Abilities (KSAs)*** are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training.
  Knowledge is a body of information applied directly to the performance of a function.
  Skill is often defined as an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cybersecurity rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual.
  Ability is a competence to perform an observable behaviour or a behaviour that results in an observable product.
- ***Tasks*** make up a specific defined piece of work that, combined with other identified Tasks, contribute to the work in a specific speciality area or work role.

We find the e-Competence Framework follows a similar logic to NICE, though in much more generalist terms and covers a broader area. Most of the reviewed documents describe skills at a rather high level, and we could in fact treat Knowledge, Skills, Abilities (differentiated by NICE) as fitting the single term “skills” – something that one learns and knows how to apply.

With the exception of NICE, these documents describe skills in quite general terms, which allows broad coverage, but provides very limited insight into the detailed content. This reduces their applicability, as in each case the same description can be granulated in a different way. On the other hand, too detailed granulation makes the framework very complex and difficult to use. Thus, balancing of skills granularity is one of the key challenges in making the SPARTA Framework effective in dealing with the requirements of the EU environment.

As mentioned in 1.4 “Applicability beyond SPARTA project”, one of the key expectations for the SPARTA Skills Framework is applicability for study programs and professional training. Applicability in the context of skills can be described as a granularity of skill description. This can be done by detailing on the level of skills (e.g. from basic to expert) or by detailing the knowledge itself (e.g. knowledge of computer network defence versus knowledge of obfuscation techniques, intrusion sets, common attack vectors on the network layer, etc.)

Overall, we found that the NICE categorization of Knowledge, Skills, and Abilities by means of fine details describing their respective features is the most practical and powerful approach, which should be leveraged further.

3.4 Identification of best practices in classification of roles and skills in the field of cybersecurity

As discussed earlier, the aim of our document review was to identify best practices that could serve as a basis for a SPARTA Cybersecurity Skills Framework.

For the definition of bests practices in the present context four criteria were applied:

- Relevance of structure – how skills and roles structures can be used for a cybersecurity skills framework. This mainly concerns links between the description of performed activities and functions and skills required for this performance. Interconnected structures were evaluated as opposed to separated structures.
- Applicability – how taxonomies and links can be used for education / professional training curriculum development and skills management systems in business organizations.
- Granularity – how descriptive are definitions of roles and skills at detailed levels.
- Sustainability – ownership of the taxonomies. Project-based structures were considered less sustainable compared to those provided by enduring organizations. Aiming to create value

beyond the project, we searched for structures, where our inputs can be used later by relevant organizations. European inputs were also valued better compared to non-EU.

The best practice identification process resulted in the selection of two frameworks for consideration:

- JRC taxonomy, as a classifier of the cybersecurity domain, made a specific effort to include the European Union landscape. The JRC taxonomy is recognised by the SPARTA project for its applicability in the cybersecurity field and relating it to the cybersecurity skills framework can benefit sustainability of both the JRC taxonomy and the SPARTA cybersecurity skills framework. Thus, any EU developed cybersecurity skills framework should be designed in a way that includes all skills relevant to the identified scope of the JRC taxonomy.
- NICE Framework, as a workforce development-oriented model, provides extensive granularity and has been developed as an instrument for academia and industry. While it can be used as a backbone for the EU based cybersecurity skills framework, it has to be modified in ways that include all JRC taxonomy defined cybersecurity categories.

Chapter 4 SPARTA Cybersecurity Skills Framework development

4.1 The SPARTA CSF Development Approach

While analysing cybersecurity skills classifications and applications in different countries, we formulated the principles which should guide the development of the new SPARTA CS Framework.

- EU clearly lags behind with the development of a comprehensive approach to defining a set of roles and skills relevant to securing organizations in the cyber field. While in some areas, like GDPR, EU demonstrates a very strong lead, we believe that progress is fastest when knowledge and experience are shared, reused and improved, rather than reinvented. Thus, we aim to reuse best practices adopting them to specific needs.
- EU focus. Though cybersecurity is an international and deeply technical phenomenon, and is not bound to national states, nevertheless, some specifics do exist. These mainly arise from legislative differences. In developing the SPARTA CS Framework, we will aim to respect EU specificities enabling frictionless use of the framework in the EU environment.
- Balancing different needs of the Member States. Member States might have their specific needs that may or may not be addressable in the EU framework. Determining balanced needs will ensure that the EU framework is universally applicable within its borders, and a common denominator will address national specificities. The Framework must not leave room for development of various national skills frameworks, as these would be counterproductive to the purpose of this pan-European enterprise.
- Current vs Future. Skills frameworks are usually developed from the standpoint of the current situation. But we find in areas of rapid progress such as cybersecurity, that emerging skills need to be taken into account. Indeed, the Framework needs to have the capability to grasp emerging trends and corresponding emerging skills. Very slow adoption of the research, concepts, technologies to the curricula of universities creates a reality where students are taught subjects rooted in the past. Conscious incorporation of the emerging trends is needed to initiate a change in the process.
- Sustainability. Strong governance is a key to adoption and continued relevance. A Governance framework has to ensure that stakeholders actively and constantly participate in efforts to ensure usage of the framework as widely as possible, so it is relevant for everyday life of people, organizations and institutions. At the same time, governance structures must ensure wide harvesting of the changes in the current approaches and future outlook of threats, so that these changes are properly reflected in the framework.
- The Member States must have a say in the governance structure to ensure their buy-in. So, discussions of the governance should consider points of view of all stakeholders (Member States being one), rather than purely functional development of the knowledge in the discussed area.

4.2 Versioning of SPARTA CS Framework

To clarify and streamline the development of SPARTA CSF, we now turn to the logic of the versioning approach that will be used.

Version numbers	Comment
0	Version 0 is the starting version which is equivalent to the source framework. Thus, it will be referred to as SPARTA CSF v0 / NICE. As in Development Step 1, the NICE Framework has been selected as a source framework, SPARTA CSF v0 is equivalent to the NICE Framework (NIST Special Publication 800-181).
0.5	Version 0 further is amended with EU specifics and other contributions, as a result working version 0.5 is developed.
0.9	After validating version 0.5 in the workshop and modifying it with inputs from T-Shark and other sources, version 0.9 is developed and presented in this document.
1.x	In further chapters, the path to develop 1.x versions is presented, including a very lean governance structure. Versions 1.x will be in continuous development until the end of the project and will be used to address the needs of the SPARTA Project
2.x	Towards the end of the project (or earlier if feasible), a SPARTA Roadmap Workshop will be held to further wider use and provide robust governance.

Table 6: Description of SPARTA Framework versions

4.3 Development Step 1: Selecting basis of SPARTA CS Framework

Review of international practice revealed that NICE is a workforce development-oriented framework which has proven its practical applicability not only in the US, but also in other countries across the globe, and thus forms a solid base to build on. But it also needs to be tested further, if its current limitations are to be overcome.

We employed the NICE Framework as a basis for the SPARTA CS Framework and undertook further work to modify it to fit SPARTA defined aims and wider EU needs. Chapter 5 discusses how the developed framework was tested to determine its relevance and applicability to the EU environment.

4.4 Development Step 2: Consolidation of JRC Taxonomy and NICE Framework

One of the goals of SPARTA Project's Work Package WP9 is to prepare a usable practical classification to:

- describe educational programs across and outside EU in the field of cybersecurity;
- to identify workforce development gaps - what knowledge areas are present and which ones are lacking in educational programs;
- to provide a practical tool for education planners as to how to comprehend existing gaps and how to modify educational programs to respond to these gaps;
- to provide tools for discussion of the knowledge and skills which will be required with the emergence of new challenges and new technologies.

The documentary analysis showed that while the JRC taxonomy provides an actual classification of the cybersecurity domain with the European union landscape, it lacks instruments that would allow such practical analysis of workforce knowledge gaps and input to educational programs.

The NICE Framework provides a very practical and applicable model of discussing roles, and knowledge/skills/abilities, but as the framework was developed in the USA, it does not cover legislative and practical aspects of cybersecurity in the EU.

By mapping the JRC taxonomy to the NICE Framework we aim to create a synergy of frameworks, thereby leveraging their specific strengths and discovering their shortcomings. This joint framework will be used further for the practical analysis of educational programs and discussion of the SPARTA technical work packages (like Research Programme #1 T-SHARK-Full spectrum cybersecurity awareness), as well as current and future knowledge needs.

4.4.1 JRC Taxonomy –NICE Framework mapping

L3CE experts performed a systematic analysis and mapping of the JRC and NICE Frameworks.

The NICE workforce development model has been selected as a basis for the classification of roles and skills, while the JRC taxonomy has been taken as a primary model to classify the cybersecurity field as a whole.

For mapping purposes, CYBERSECURITY DOMAINS dimension of the JRC taxonomy was used at the level of subdomains to retrieve the highest level of detail. It was decided to focus solely on the JRC Cybersecurity Domains axis in this mapping effort, to map them to NICE work roles.

Technology and Applications being the technical tools, from the perspective of workforce development, which would be relevant in relation to tasks of the roles and knowledge of instruments, which roles must have.

Industries do provide their specificities, but they are not relevant at this stage as the cybersecurity skills framework covers all the work roles inherent in the cybersecurity domain. This field is not EU/USA specific and further mapping and expanding the skills framework should rely on development through the governance process.

Experts analysed in detail the JRC taxonomy Cybersecurity Domains within the subdomain level. During this effort, every JRC taxonomy SUBDOMAIN that corresponded to WORK ROLES from NICE was selected, and this revealed a significant contribution. An effort was made to list every relevant Work Role, though sometimes it proved to be more feasible to map higher-level groups as Specialty Areas (containing several roles) or Categories (containing several Specialty Areas).

The mapping effort is documented in detail in Annex 1   Mapping of JRC taxonomy and NICE Framework". Every JRC domain is mapped to specific NICE work roles, and observations are documented.

4.4.2 Observations of JRC Taxonomy – NICE Framework mapping

The table below summarizes the mapping of JRC Cybersecurity Domains onto the subdomains level of the NICE Framework Specialty Areas (In Annex 1, detailed demonstration of the mapping to specific Work Roles is documented).

JRC taxonomy subdomains	NICE Framework						
Subdomains	Securely provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)	Investigate (IN)
Assurance, Audit, and Certification	X		X	X			
Data Security and Privacy	X	X	X				
Education and Training			X				
Operational Incident Handling and Digital Forensics							X
Human Aspects	X		X	X	X	X	

JRC taxonomy subdomains	NICE Framework						
Subdomains	**Securely provision (SP)**	**Operate and Maintain (OM)**	**Oversee and Govern (OV)**	**Protect and Defend (PR)**	**Analyze (AN)**	**Collect and Operate (CO)**	**Investigate (IN)**
Identity and Access Management (IAM)	X	X	X				
Security Management and Governance	X	X	X	X	X	X	
Network and Distributed Systems	X	X	X	X		X	
Software and Hardware Security Engineering	X						
Security Measurements	X						
Legal Aspects			X		X		X
Theoretical Foundations	X		X				
Trust Management, Assurance, and Accountability	X		X		X	X	

Table 7: JRC Taxonomy and Nice Framework mapping

During the mapping exercise, the following observations were noted:

- JRC taxonomy and NICE Framework aim to classify areas of cybersecurity from substantially different angles and at a different abstraction level. It is obvious that mapping the JRC taxonomy and NICE Framework is far from straightforward. Further analysis and conceptualizing effort are needed to ensure comprehensive mapping with all vectors of the JRC taxonomy.
- JRC taxonomy and skills framework mapping is a valuable exercise that can uncover “blind spots” and can be valuable for both frameworks as the cybersecurity field develops.
- Some suggestions emerged as to how to make the JRC taxonomy more consistent from the standpoint of practical application. These considerations were further presented for validation by stakeholders.
- While the NICE Framework covers all roles for the JRC taxonomy domains, it became obvious that the EU legislative environment dictates roles, namely that of GDPR, which does not fit straightforwardly into the framework’s existing roles structure.

The JRC Taxonomy and NICE Framework mapping exercise have resulted in the recognition that the NICE Framework can serve as a solid basis for SPARTA Cybersecurity Skills Framework development, as all JRC cybersecurity/research domains seem to be covered. We have to admit that however the EU landscape may be amended, the SPARTA CS Framework will continue to be a valuable instrument for achieving the aid of effective cyber workforce development.

At this stage, SPARTA CSF version 0 is constituted as a copy of the NICE Framework (NIST Special Publication 800-181), and SPARTA CSF version 0 is developed into later versions, which are further described in this document.

4.5 Development step 3: Amending SPARTA CS Framework with EU landscape

The documentary analysis identified that the NICE Framework has strong US ties, and lack of coverage of the EU landscape has been pointed out as a significant NICE Framework drawback in a number of documents. The analysis revealed that on the question of cybersecurity skills, the United States and the European Union do not differ in their respective approaches to technological or applicability areas. Significant differences, however, are revealed when considering the regulatory domain.

4.5.1 Adapting to EU legal framework

We incorporated the EU legal landscape into the SPARTA CS Framework v0 while aiming to preserve its integrity. The three areas of special significance identified in this context are listed below:

- Adapting to EU level regulations, namely GDPR
- Realigning Framework references to the relevant EU legal documents
- Introducing into the framework roles legislated in the Member State.

4.5.1.1 EU level legal regulations

GDPR is an EU related framework for personal data protection, was not specifically covered in the NICE Framework. Lack of EU relevance is very often encountered as a critique of the applicability of the NICE Framework in the European context.

Furthermore, with the introduction of GDPR, the EU put the protection of personal interests of the data subject in the forefront of its concerns, and in the face of significant fines and a strong supervisory regime, organizations are motivated to be compliant. In the US, however, the approach varies from state to state, with the major concern being cybersecurity and data integrity, rather than personal privacy. The US implements sector-specific federal legislation which works together with state laws (e.g. HIPAA for health information, and NIST800-171 for protecting Controlled Unclassified Information (CUI) in non-federal information systems and organizations).

Overall, in light of EU's much stronger focus on protecting the personal interests of the data subject, we feel that this aspect needs to be strongly reflected in the EU skills framework.

As the Sparta CS Framework is based on the NICE Framework, in order to establish its validity within the EU environment, the framework must be amended, and so we now describe the method used.

GDPR defines entities (natural or legal persons) that control or process personal data as being directly accountable for personal data protection, and as such GDPR legislation requires that these entities comply with the rules of personal data protection. Companies and organizations, satisfying specific criteria defined in GDPR, must appoint a Data Protection Officer (DPO) who in this role is charged with specifically defined responsibilities related to the compliance process.

In conclusion, the SPARTA CS Framework should ensure that GDPR is reflected in the framework both in the case in which a formal role of Data Protection Officer is put in place by an organization or in the case when an entity may not have the resources to support such a formal role. Nevertheless, in both cases, compliance with GDPR requirements is mandatory.

4.5.1.2 Data Protection Officer (DPO) Role Definition

This is an organization role, which is responsible for overseeing an organization's data protection strategy and implementation. The DPO should also be involved properly, and in a timely manner, in all issues, which relate to the protection of personal data (Article 38[18]). According to Article 38, no one in the organization is allowed to issue any instructions to DPOs regarding the performance of their tasks. In addition, he or she has to meet confidentiality requirements and report directly to the highest management level of the organization.

A Data Protection Officer according to Article 39[19] has five major responsibilities:

- To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or the Member State data protection provisions;
- To monitor compliance with this Regulation, with other Union or the Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35[20];
- To cooperate with the supervisory authority;
- To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36[21], and to consult, where appropriate, with regard to any other matter.

A related work role in the NICE Framework is the role of the Privacy Officer. In this role, a person develops and oversees the privacy compliance program and engages in the development of staff competencies, supports privacy compliance efforts, develops governance/policy, and participates in incident response.

In the NICE Framework, the Privacy Officer/Privacy Compliance Manager role involves the execution of an extensive set of tasks. Some of these tasks overlap with those of GDPR DPO tasks. Further, in the table below, the reader can find all GDPR DPO Tasks mapped to the corresponding tasks delineated in SPARTA CSF v0 / NICE.

For reference, the SPARTA CSF v0 / NICE full task list of this role can be found in Annex 2 Task list of NICE Privacy Officer/Privacy Compliance Manager role".

Task No.	GDPR DPO Tasks	NICE Framework role "Privacy Officer/Privacy Compliance Manager Tasks"
1.	To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;	T0880 – Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations; T0881 – Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties;

[18] https://gdpr.eu/article-38-data-protection-officer\
[19] https://gdpr.eu/article-39-tasks-of-the-data-protection-officer/
[20] https://gdpr.eu/article-35-impact-assessment/
[21] https://gdpr.eu/article-36-supervisory-authority-consultation/

Task No.	GDPR DPO Tasks	NICE Framework role "Privacy Officer/Privacy Compliance Manager Tasks"
		T0882 – Conduct on-going privacy training and awareness activities.
2.	To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;	T0032 - Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII); T0188 – Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions;
3.	To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35[3];	T0862 – Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements; T0865 – Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues;
4.	To cooperate with the supervisory authority;	T0861 – Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations;
5.	To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36[4], and to consult, where appropriate, with regard to any other matter.	T0871 – Collaborate on cyber privacy and security policies and procedures; T0872 – Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation;

Table 8: The overlapping DPO and Privacy Officer tasks

The analysis shows that SPARTA CSF v0 / NICE Framework defined "Privacy Officer/Privacy Compliance Manager" work role broadly covers the GDPR Data Protection Officer role's tasks.

But due to the fact that GDPR defines the Data Protection Officer very clearly as a separate role, which requires special reporting, etc., for the purposes of clarity and systematic representation in our skills matrix, the Data Protection Officer (GDPR) should be added as a separate work role.

This decision was validated in the workshop.

4.5.1.3 Other roles

It is important to mention that GDPR defines the broad responsibilities of personal data controllers and processors. The Data Protection Officer has a formal and mostly advisory work role that encompasses only a subset of these responsibilities.

So, as personal data protection constitutes a major liability in the cybersecurity space of an operating organizational entity, we find it necessary to amend the description of roles to strengthen the weight of privacy. In framing roles that bear general responsibility for planning and complying with GDPR requirements, organizations will have to have a clear understanding of the necessities to comply (even though they may not have formally included the Data Protection Officer role in their organization).

Here are two examples of roles we modified to include “privacy” in the working title and the description:

> **Cyber / Privacy Policy and Strategy Planner** - Develops and maintains cybersecurity/privacy plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
>
> **Executive Cyber / Privacy Leadership** - Has decision-making authority and establishes vision and direction for an organization's privacy, cyber and cyber-related resources and/or operations.

4.5.1.4 SPARTA CSF v0 / NICE Framework realigning to EU context

United State of America national-focused areas

The NICE Cybersecurity Workforce Framework (NICE Framework), is a national-focused resource developed in the USA that categorizes and describes cybersecurity work. SPARTA is creating a new Cybersecurity Skills Framework, which needs to take into account European law.

The adaptation process started from the identification of all aspects which were either directly or indirectly linked with U.S. law, and to adapt them to European law.

To identify the areas in the NICE Framework, which were U.S. Law specific, we analyzed roles and related knowledge groupings. The tables below exhibit the results of this analysis.

In the table below, we selected items of identified knowledge from SPARTA CSF v0 / NICE which refer directly to the legislation of US origin.

K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).
K0066	Knowledge of Privacy Impact Assessments.
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.
K0262	Knowledge of Personal Health Information (PHI) data security standards.

Table 9: U.S. Law specific knowledge components (Source: https://doi.org/10.6028/NIST.SP.800-181)

In the table below we selected roles from SPARTA CSF v0/ NICE which have a direct reference to legislation or documents of US origin.

Authorizing Official/Designating Representative	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009[22]).
Security Control Assessor	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
Communications Security (COMSEC) Manager	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).

Table 10: U.S. regulation specific Roles (Source: https://doi.org/10.6028/NIST.SP.800-181)

4.5.1.5 Adoption of EU rules and regulations context to SPARTA Framework

After the identification of the areas which should be modified to meet the EU specific context, the analysis of EU regulations and Laws was undertaken. The outcome of this analysis identified the EU laws which are similar to U.S. Laws.

In the table below, we define knowledge-based on US law and documents and provide modifications to the SPARTA CSF to realign corresponding items to the EU landscape.

U.S. Law specific	EU Specific
Knowledge of information security systems engineering principles (NIST SP 800-160).	Knowledge of information security systems engineering principles (NIS directive[23])
Knowledge of Privacy Impact Assessments.	Knowledge of Privacy Impact Assessments (e.g. Data Protection Impact Assessment (DPIA)[24]).
Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Knowledge of national legal acts related to admissibility.
Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Knowledge of Supply Chain Risk Management Practices (e.g. INT/681-EESC-2013-1653[25])
Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Knowledge of EU Law's, directives, Regulations, Decisions, Recommendations, Opinions[26].
Knowledge of Personally Identifiable Information (PII) data security standards.	Knowledge of General Data Protection Regulation (GDPR)[27].

[22] https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

[23] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[24] https://gdpr.eu/data-protection-impact-assessment-template/

[25] https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/risk-management-security-supply-chain

[26] https://europa.eu/european-union/eu-law/legal-acts_en

[27] https://gdpr.eu/tag/gdpr/

Knowledge of Personal Health Information (PHI) data security standards.	Knowledge of the General Data Protection Regulation (GDPR)[28] directive definition for health data for data protection purposes.

Table 11: Knowledge adaptation to EU legislative landscape

Role:	U.S. Law specific	EU specific
Authorizing Official/Designating Representative	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (NIS Directive).
Security Control Assessor	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (i.e. as described in NIS Directive).
Communications Security (COMSEC) Manager	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).	Individual who manages the Communications Security (COMSEC) resources of an organization (NIS Directive) or key custodian for a Crypto Key Management System (CKMS).

Table 12: Adaptation of Roles to reflect EU regulations

In the table below, we define Work Roles having references to US law and documents and provide modifications to the SPARTA CSF to realign the corresponding items to the EU landscape.

4.5.1.6 Guidelines for further development

We find that the current definition of knowledge in “Knowledge of EU Law’s, directives, Regulations, Decisions, Recommendations, Opinions” is much too general. It should be expanded and refined so as to include major aspects that cybersecurity experts should have knowledge of.

Concerning the issue of “Knowledge of national legal acts related to admissibility,” there is no EU wide legislation regarding admissibility in relation to cybercrimes, thus professionals will have to rely on national guidelines. This is a perfect example of national regulation which in some way has to

[28] https://gdpr.eu/recital-35-health-data/

enter the purview of the Framework, thus extensive discussions will be needed to determine how such national regulations can or should be reflected in the body of the Framework.

Furthermore, realignment effort specifically with GDPR demonstrated that some legislative approaches are different in very substantial ways between US and EU, so more analysis may be needed in this area.

4.5.1.7 National level legal regulations

Documentary analysis of the situation in Lithuania revealed that national legislation somewhat vaguely defines a cybersecurity (or cyber-safety) manager (in Lithuanian: “Saugos įgaliotinis“) role in general terms as a person who is responsible for the secure (or safe) operations of the governmental system in question.

This specific example demonstrates the case that the Member State legislation may have some relevance to the Framework and this is expected to be defined on a case by case basis, without a uniform scenario.

Thus, there remains an open question: should the framework try to incorporate roles stemming from the Member State legislation, and if it should, then how is it to be undertaken? This question was further addressed in the validation workshop described in the Chapter which follows.

Chapter 5 Validation of SPARTA CS Framework v0.5

5.1 Validation workshop

Chapter 4 described how the SPARTA Cybersecurity Skills Framework version 0.5 was developed (0.x versions are in the development stage, for discussion purposes only, as described in Table 6). The NICE Framework was selected as a basis to work from, and the skills framework was reviewed and adapted to the EU context; after changes and amendments were made, the 0.5 version was produced.

This version was peer-reviewed by L3CE experts.

To test the relevance of the newly developed SPARTA CS Framework, a workshop of SPARTA stakeholders was organized.

Agenda of the workshop was focused on three main topics:

- Inclusion of EU specific legislation into the Framework;
- Applicability - test if the provided Framework provides value for academia by i) facilitating analysis of existing curricula, ii) guiding efforts for the enriching of curricula with necessary skills, and for industry by helping to analyse actual roles and their skillset in the organization;
- Adaptability – the ability of the Framework to include and provide a clear indication of emerging roles and skills, required for cybersecurity operations in the near future (based on predictions, provided by the T-SHARK Programs within the SPARTA project).

The workshop was attended by representatives of the SPARTA project partners and external quests.

5.2 Validation of EU landscape

As described in the discussion in Chapter 4, the NICE Framework, which adds significant input to the SPARTA CS Framework, clearly lacks the EU landscape, and thus fails to incorporate specificities of the EU regulatory environment, is not synchronized with the Member State realities, and is based on the US legislative context.

In preparing the Sparta CS Framework, the authors adopted certain modifications which should have eliminated the aforementioned bias and developed a skills matrix that is based on the EU legislative environment and realities of the Member States.

- Aims of EU landscape validation were to determine if the SPARTA CS Framework is capable of including EU specificities;
- Able to grasp specificities of the Member State cybersecurity-related legislation.

Participants were presented with the challenge of how the role of Data Protection Officer described in GDPR legislation is to be added to the SPARTA CS Framework.

Amendments were presented which related to EU legislation, rules and regulations.

The case of Lithuanian cybersecurity legislation which defines the role of “Saugos Įgaliotinis“ (cybersecurity or cyber-safety manager) was presented.

5.2.1 Results of the validation of EU landscape

Participants of the workshop confirmed that the Data Protection Officer has to be represented as a separate role in the skills matrix due to its very clearly and strictly being defined in EU legislation.

Participants agreed that references to US documents have to be removed and EU documents have to be amended. Due to contextual differences with the US approach, considered changes cannot be limited to solely providing references to the EU document. EU context has to be analysed to consider the entire scope of the relevant EU rules and regulations which cybersecurity roles have to take into account. This effort has to continue in the ongoing stages of development of the Framework.

Participants confirmed the notion that an EU wide framework should be limited to commonalities of EU, rather than focus on specificities of the Member States. On the other hand, it is very important to have one Framework for all EU Member States, rather than many modified ones spread across Europe. Due to the lack of a comprehensive analysis of specific legislation associated with the various Member States, experts upheld the notion that most of the specificities would be accommodated by the existing definitions of roles. Further discussions and adoptions might be necessary in this regard.

5.3 Applicability validation

One of the most relevant critiques of the various frameworks encountered in the analysis was “applicability”. In every single case, there was a discussion as to whether the framework in question is too abstract to provide any practical value (failing to provide any prescription, abstractions encompassing everything, etc.), or too detailed, making documents incomprehensible and unmanageable for practitioners.

During the workshop, the results of the applicability exercises were presented.

Prior to the workshop exercises were provided to representatives of academia with a request to fill in the questionnaire.

Two exercises were provided to the representatives from academia who had the first-hand experience in analysis and development of curricula.

The aim of the academia applicability exercise was to test if the provided cybersecurity skills framework meets the following criteria:

- Has the power to facilitate analysis of existing curricula;
- Is capable of guiding efforts for an enriching skill-related curricula.

The purpose of the industry exercise was to validate the applicability of SPARTA cybersecurity skills framework to the analysis of the actual roles and their skillset in the organization.

5.3.1 Results of applicability validation

Participants from academia agreed that the provided framework is useful to analyse and amend the curricula of the universities. They also found it helpful to analyse comprehensiveness of curricula where knowledge elements of the university's programs were missing.

During the discussion, concerns were raised that the framework was too dense, but afterwards, the participants were in agreement that the overall granularity of the framework is highly practical.

Industry experts who were asked to fill in the questionnaire were unable to respond in good time and did not participate in the workshop. Thus, validation by industry is still pending and will be undertaken in the January – February time frame.

5.4 Adaptability validation

To validate the capacity of the Framework for adaptability, in-depth interviews with T-Shark experts were held. The Framework was presented, and the overall structure was discussed. During these interviews, attempts were made to determine how the Framework reflects aspects of T-Shark or fails to do so.

In principle, it was agreed that currently required skills are well grasped in the Framework, but that some of the aspects specific to complex threats, trends or emerging threats are covered only partially.

The following observations were recorded:

- The current focus in cybersecurity is mainly on technical aspects, while comprehensive cybersecurity requires a wider scope. Information security, situational awareness, relationship of kinetic and cyber environments are becoming increasingly important.
- While security within the internal perimeter has been considered as a core of cybersecurity, today there is a need to handle and secure infrastructures outside the organization. Social media platforms are a good example of such expansion.
- Understanding and inclusion of much wider threats to the cybersecurity landscape is needed. The current focus is on incidents, which make up only a part of the bigger picture.
- It is important to move from being a responsive organization to CS threats towards more predictive and proactive activities.
- There are other implications such as changing modus operandi in CS, like new technologies (e.g. quantum and post-quantum computing, automated incident response, ML based and big data-dependent solutions, etc.), or extended data exchange and data source management, or wider risk types to be handled.

These changes have complex implications in relation to all components of the Framework - Tasks to be handled, functions to be described and KSAs required.

5.4.1 Results of adaptability validation

T-Shark experts and participants of the workshop agreed that the Framework demonstrated a strong basis for adaptability to the new trends and capacity to expand accordingly.

Participants noted that it is highly important to ensure the integrity of the Framework by not allowing arbitrary amendments to be introduced which would destroy the internal structure of the Framework. Thus, new trends deemed to be of significance have to enter into the framework in a well-defined manner, passing the necessary vetting mechanisms.

5.5 Other aspects of validation

During the workshop, specific attention was paid to the question of granularity. At first, users were seemingly confronted with an overwhelming document. But after the analysis and practise sessions, the participants agreed that the Framework provides the right balance to be useful for practical work.

SPARTA Work Package 9 representatives agreed on the usefulness of the Framework for analysis and development of curricula and suggested that the Framework should be integrated with the categorization already used for T9.2 and T9.3 analysis efforts.

The ECSO representative noted that they had analysed potential frameworks and came to the same conclusion, that the NIST NICE Framework is the best starting point for the development of a comprehensive cybersecurity skills matrix.

Chapter 6 SPARTA Cybersecurity Skills Framework v0.9

Initial development of the SPARTA CS Framework in multiple reiterations resulted in version 0.9 (non-public version, for discussion purposes only) which is further described here.

6.1 Description of the Framework

Here, we will present the high-level structure of the Framework and relevant differences between it and the SPARTA CSF v0 / NICE Framework (NIST Special Publication 800-181).

6.1.1 Structure

The structure of the Framework remains the same as in the NICE Framework and consists of three levels:

- Categories
- Specialty areas
- Work roles

Work roles can be broken down further into various attributes, including tasks and knowledge elements.

6.1.1.1 Categories

There are seven Categories which are composed of Specialty Areas and work roles. This organizational structure groups together work and workers that share common major functions, regardless of job titles or other occupational terms.

The structure of Categories and of Specialty areas of the SPARTA CS Framework v0.9 remains unchanged compared to the NICE Framework (NIST Special Publication 800-181).

Categories	Descriptions
Securely Provision SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Table 13: Alignment of SPARTA Framework Categories with NICE Framework Categories (Primary source: https://doi.org/10.6028/NIST.SP.800-181)

6.1.1.2 Specialty areas

Categories contain groupings of cybersecurity work, which are called Specialty Areas. Each specialty area represents an area of concentrated work, or function, within cybersecurity and related work.

Specialty areas of the SPARTA CS Framework v0.9 remain unchanged compared to the NICE Framework (NIST Special Publication 800-181) Specialty areas.

Categories	Specialty Areas	Specialty Area Descriptions
Securely Provision (SP)	Risk Management (RSK)	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
	Software Development (DEV)	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
	Systems Architecture (ARC)	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
	Technology R&D (TRD)	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
	Systems Requirements Planning (SRP)	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
	Test and Evaluation (TST)	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost- effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.
	Systems Development (SYS)	Works on the development phases of the systems development life cycle.
Operate and Maintain (OM)	Data Administration (DTA)	Develops and administers databases and/or data management systems that allow for the storage, query, protection, and utilization of data.
	Knowledge Management (KMG)	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Customer Service and Technical Support (STS)	Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response (IR) Specialty.
	Network Services (NET)	Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
	Systems Administration (ADM)	Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Manages accounts,

Categories	Specialty Areas	Specialty Area Descriptions
		firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
	Systems Analysis (ANA)	Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively. Brings business and information technology (IT) together by understanding the needs and limitations of both.
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
	Training, Education, and Awareness (TEA)	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.
	Cybersecurity Management (MGT)	Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.
	Strategic Planning and Policy (SPP)	Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.
	Executive Cyber Leadership (EXL)	Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.
	Program/Project Management (PMA) and Acquisition	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.
Protect and Defend (PR)	Cyber Defense Analysis (CDA)	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.
	Cyber Defense Infrastructure Support (INF)	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.
	Incident Response (CIR)	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
	Vulnerability Assessment and Management (VAM)	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
Analyze (AN)	Threat Analysis (TWA)	Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces

Categories	Specialty Areas	Specialty Area Descriptions
		findings to help initialize or support law enforcement and counterintelligence investigations or activities.
	Exploitation Analysis (EXP)	Analyzes collected information to identify vulnerabilities and potential for exploitation.
	All-Source Analysis (ASA)	Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.
	Targets (TGT)	Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
	Language Analysis (LNG)	Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.
Collect and Operate (CO)	Collection Operations (CLO)	Executes collection using appropriate strategies and within the priorities established through the collection management process.
	Cyber Operational Planning (OPL)	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
	Cyber Operations (OPS)	Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
Investigate (IN)	Cyber Investigation (INV)	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
	Digital Forensics (FOR)	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

Table 14: Alignment of Speciality areas (Primary source: https://doi.org/10.6028/NIST.SP.800-181)

6.1.1.3 Work roles

Table 15 provides a description of each of the work roles.

The structure of work roles of the SPARTA CS Framework v0.9 in most cases remains unchanged compared to the NICE Framework (NIST Special Publication 800-181). Exceptions include the Data Protection Officer role and the Member State-specific role of Cyber Security Officer. EU specific work roles by adding the “EU” extension in the Work Role ID description.

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Securely Provision (SP)	Risk Management (RSK)	Authorizing Official/Designating Representative	SP-RSK-001	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets,

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
				individuals, other organizations, and the Nation (CNSSI 4009).
		Security Control Assessor	SP-RSK-002	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
	Software Development (DEV)	Software Developer	SP-DEV-001	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
		Secure Software Assessor	SP-DEV-002	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture (ARC)	Enterprise Architect	SP-ARC-001	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
		Security Architect	SP-ARC-002	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
	Technology R&D (TRD)	Research & Development Specialist	SP-TRD-001	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
	Systems Requirements Planning (SRP)	Systems Requirements Planner	SP-SRP-001	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
	Test and Evaluation (TST)	System Testing and Evaluation Specialist	SP-TST-001	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
	Systems Development (SYS)	Information Systems Security Developer	SP-SYS-001	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.
		Systems Developer	SP-SYS-002	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Operate and Maintain (OM)	Data Administration (DTA)	Database Administrator	OM-DTA-001	Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.
		Data Analyst	OM-DTA-002	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modelling, data mining, and research purposes.
	Knowledge Management (KMG)	Knowledge Manager	OM-KMG-001	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
	Customer Service and Technical Support (STS)	Technical Support Specialist	OM-STS-001	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).
	Network Services (NET)	Network Operations Specialist	OM-NET-001	Plans, implements, and operates network services/systems, to include hardware and virtual environments.
	Systems Administration (ADM)	System Administrator	OM-ADM-001	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
	Systems Analysis (ANA)	Systems Security Analyst	OM-ANA-001	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	Cyber Legal Advisor	OV-LGA-001	Provides legal advice and recommendations on relevant topics related to cyber law.
		Privacy Officer/Privacy Compliance Manager	OV-LGA-002	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
		Data Protection Officer	OV-LGA-003-EU	Responsible for overseeing an organization's data protection strategy and implementation as defined in GDPR legislation. Is involved properly and in a timely manner, in all issues, which relate

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
				to the protection of personal data. Role has full autonomy in executing its duties and reports directly to the highest management level of the organization.
	Training, Education, and Awareness (TEA)	Cyber Instructional Curriculum Developer	OV-TEA-001	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.
		Cyber Instructor	OV-TEA-002	Develops and conducts training or education of personnel within cyber domain.
		Information Systems Security Manager	OV-MGT-001	Responsible for the cybersecurity of a program, organization, system, or enclave.
		Information Systems Security Manager according to EU Member State legislation	OV-MGT-002-EU	In case the Member State has a special legislation, which describes a role of IT/Cybersecurity manager with the special roles / responsibilities, this role is described in the per Member State basis, if applicable
	Cybersecurity Management (MGT)	Communications Security (COMSEC) Manager	OV-MGT-002	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).
	Strategic Planning and Policy (SPP)	Cyber Workforce Developer and Manager	OV-SPP-001	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.
		Cyber Policy and Strategy Planner	OV-SPP-002	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
	Executive Cyber Leadership (EXL)	Executive Cyber Leadership	OV-EXL-001	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
	Program/Project Management (PMA) and Acquisition	Program Manager	OV-PMA-001	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.
		IT Project Manager	OV-PMA-002	Directly manages information technology projects.
		Product Support Manager	OV-PMA-003	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.
		IT Investment/Portfolio Manager	OV-PMA-004	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
		IT Program Auditor	OV-PMA-005	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.
Protect and Defend (PR)	Cyber Defense Analysis (CDA)	Cyber Defense Analyst	PR-CDA-001	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
	Cyber Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	PR-INF-001	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.
	Incident Response (CIR)	Cyber Defense Incident Responder	PR-CIR-001	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
	Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst	PR-VAM-001	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Analyze (AN)	Threat Analysis (TWA)	Threat/Warning Analyst	AN-TWA-001	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
	Exploitation Analysis (EXP)	Exploitation Analyst	AN-EXP-001	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.
	All-Source Analysis (ASA)	All-Source Analyst	AN-ASA-001	Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.
		Mission Assessment Specialist	AN-ASA-002	Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.
	Targets (TGT)	Target Developer	AN-TGT-001	Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
				intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.
		Target Network Analyst	AN-TGT-002	Conducts advanced analysis of collection and open- source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.
	Language Analysis (LNG)	Multi-Disciplined Language Analyst	AN-LNG-001	Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.
Collect and Operate (CO)	Collection Operations (CLO)	All Source-Collection Manager	CO-CLO-001	Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.
		All Source-Collection Requirements Manager	CO-CLO-002	Evaluates collection operations and develops effects- based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.
	Cyber Operational Planning (OPL)	Cyber Intel Planner	CO-OPL-001	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

		Cyber Ops Planner	CO-OPL-002	Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.
		Partner Integration Planner	CO-OPL-003	Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.
	Cyber Operations (OPS)	Cyber Operator	CO-OPS-001	Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.
	Cyber Investigation (INV)	Cyber Crime Investigator	IN-INV-001	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.
	Digital Forensics (FOR)	Law Enforcement/Counterintelligence Forensics Analyst	IN-FOR-001	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.
		Cyber Defense Forensics Analyst	IN-FOR-002	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Table 15: Description of each of the work roles (Primary source: https://doi.org/10.6028/NIST.SP.800-181)

6.1.1.4 Knowledge, Skills, Abilities

Work roles in the framework are mapped with Knowledge, Skills and Abilities.

Knowledge, skills and abilities of SPARTA CS Framework v0.9 in most cases remain unchanged compare to the NICE Framework (NIST Special Publication 800-181) KSAs.

Respective changes are made in SPARTA CS Framework v0.9 Excel format that can be provided for further development.

6.2 Uses of the Framework

In this chapter application of the Framework for academia and industry is described, highlighting the value this complex framework can bring to the entity. Academia and industry use are described separately, as application and benefits are rather different.

Usability description is based on the validation activities (Chapter 5 Validation of SPARTA CS Framework v0.5) which were executed in a limited scope, and at this stage are open for further validation efforts and resulting adjustments.

The Framework can be used by Academia in many different ways, but the main uses identified are as follows:

- Evaluate – the right granularity of requested knowledge/abilities / skills allows education and training providers to review their curricula in a structured and systematic manner. They have a recognised framework to be used as the main benchmark instrument.
- Improve – can be done based on the evaluation exercise. This is especially important considering the emerging needs of practitioners. The Framework is able to transmit arising requests at an early stage, providing academia with the foresight to improve and develop their curricula further.
- Focus –education provided by universities may differ in the way they focus on core competencies. Some might be more focused on specific technological subjects, some on law, others on forensics, etc. Having an integrated Framework to work with, they can map their core competencies onto various subject areas, important for defined Roles. This enables the institution to develop more effective targeted programs in house around the main competencies.

Industry can use the Framework from different perspectives. It can provide a corporate entity with insights on:

- Relevance – having the full description of cybersecurity functions and activities (described as Roles), the organization can evaluate relevance of those functions. For example, planning and implementation of offensive cybersecurity activities will be irrelevant for most of SME's, while some other functions can appear as relevant, but not be included in the organization's daily activities. The Framework allows the organization to define the complete relevant scope of cybersecurity roles.
- Capacity – if relevant functions are defined, the organization can evaluate its capacity to perform them. Having a clear description of needed KSA's, it becomes easier to make decisions on outsourcing, training and evaluation of respective specialists.
- Management – the framework, if it is structured in the same manner as any typical skills management system, can be directly integrated into the system, and used by the business organization.

The current state of the Framework, as a very complex tool, can be less useful for small entities. But it also provides a lot of room for improvement and includes specific features for SME's, policymakers, etc.

6.3 Further development of SPARTA CS Framework during the SPARTA project

SPARTA CS Framework development efforts should be viewed in the context and timeline of the SPARTA project. At the time of presenting this document and SPARTA CS Framework version 0.9 (non-public, for discussion purposes only release), the SPARTA project has been operational for one year and has two more years to complete.

The T9.1 team plans activities for further development of the SPARTA CS Framework in order to validate and test it with a broad audience of stakeholders. It is intended that SPARTA CSF version 1.x will be for internal use only (i.e. for validation and testing purposes of the SPARTA project).

Depending on the validation outcomes, feedback on acceptance and relevance of the SPARTA CSF, this framework might be prepared and published for public use (SPARTA CSF versions 2.x).

Over the next two years, we will be preoccupied with on-going activities and dealing with critical decision points for the successful execution of the SPARTA project.

6.3.1 Development of SPARTA CSF versions 1.x

As discussed in earlier chapters from the basis of the NICE Framework, the SPARTA CS framework was developed up to version 0.9. Then, SPARTA CSF was modified to include the EU landscape and validated as to its applicability and adaptability. As a result, SPARTA CSF v0.9 represents a current snapshot of skills required for workforces to deal with the challenges of securing organizations.

The ambition for the development of the cybersecurity skills framework was to define not only current skills necessary to secure organizations but to also include trends in the emerging skills required, based on emerging threats and technologies. Testing of Adaptability revealed some significant trends which should find their way into the SPARTA CSF. But if this task was to be handled by several self-appointed experts, the whole framework may end up lacking in credibility.

T9.1 team came to the conclusion that the task of updating the SPARTA CS Framework with skills based on emerging trends, while sustaining the integrity of the Framework, requires a functioning update process.

Further development of the SPARTA CS Framework version 1.x (for SPARTA use) should include the following suggested approach:

1. The SPARTA Joint Centre of Competence Infrastructure (JCCI) will assign Framework Experts – three top cybersecurity professionals who will act as gatekeepers of the Framework. They will have a mandate to analyse inputs and to approve updates.
2. JCCI will assign five participants who will function as a Supervisory Board of SPARTA CSF.
3. The SPARTA WP9.1 team will serve as the Secretariat, collecting inputs from four SPARTA technical streams and providing these to experts, ensuring smooth communication and collaboration.
4. Upon receiving inputs, assigned Framework Experts will discuss and decide by unanimous agreement on which inputs should be considered for integration into the framework.
5. This process will be performed periodically up to project completion. The experience of this process will be reported and discussed and will constitute one of the important inputs for establishing a permanent governance structure.

6.3.2 Validation of SPARTA CSF

To validate the practical power of the SPARTA CSF and its applicability in different areas we will undertake a series of events that will include interviews and workshops with the executives of small and medium-sized enterprises to validate the capabilities of the SPARTA CSF.

Feedback from the validation efforts will be documented and reported to the Framework Experts and Supervisory Board for consideration.

This effort will be completed by June 2021.

6.3.3 Use of SPARTA CSF in SPARTA Project

SPARTA CSF is a deliverable to be used by T9.2 for the analysis of the cybersecurity curricula in participating Universities. This framework will serve as a common denominator for the analysis that will produce results in T9.2 and T9.3 which in turn will be communicated back to the institutions. Further, T9.2 and T9.3 will work on amending educational programs and professional training to add new skills to the curricula.

This effort will be very important as a test for applicability of the SPARTA CSF for use in academia and will provide vast practical material and feedback to Framework Experts and the Supervisory Board.

These activities will continue up to the completion of the SPARTA project.

6.3.4 Presentations

SPARTA CSF will be presented on various occasions to relevant parties/stakeholders of the project in order to raise awareness, show benefits and uses of the Framework, involve these players in the development of the Framework and strengthen the support network.

During presentations questions about relevance, governance, sustainability will be taken up to facilitate discussion, obtain differing views, and acquire buy-in. Various stakeholder groups will be involved, including but not limited to:

- Member State representatives;
- EU institutions and EC representatives associated with the field of cybersecurity;
- Other projects, etc.

Feedback from such events will be documented and will be provided to the Framework Experts and Supervisory Board for consideration.

These observations may provide important insight into the further development of sustainability/governance structures of SPARTA CSF.

This effort will continue until the completion of the SPARTA project.

6.3.5 SPARTA CSF roadmap workshop

September – October 2022 SPARTA CSF roadmap workshop will be held to decide on next steps to be taken on the cybersecurity skills development path (dates are tentative based on need; maybe scheduled sooner).

Presentations will cover the following topics:

- state of the SPARTA CSF
- lessons from the validation exercises
- input from discussions with interested parties/stakeholders
- governance of SPARTA CSF
- the possible role of SPARTA CSF in the broader context of EU and its usefulness as an EU cybersecurity skills framework.

Major decision to be taken in the workshop will be whether or not SPARTA CSF should have a development path beyond the SPARTA project. If positive, further steps will need to be taken to establish governance structures and ensure the sustainability of the framework beyond the SPARTA project.

Thus, while the CS framework is being developed by the SPARTA project, at some point down the road (which may be decided at the SPARTA CSF roadmap workshop) it should lose direct connection to SPARTA inputs. After established governance structures are functional, the SPARTA project should further provide insights and suggestions for updating the framework, but those suggestions would be reviewed and incorporated into the framework via the due process of Framework governance. Thus, no special treatment or special process of further SPARTA inputs should be considered

6.4 Governance of the Framework

We turn to a discussion on the sustainability and governance of the framework which should be thoroughly discussed with stakeholders and implemented before the end of the SPARTA Project. Further chapters are input to these discussions.

The governance of the framework incorporates an essential set of processes responsible for keeping the framework up to date, relevant and sustainable. If the framework fails to keep up with the realities, due to developments in technologies, threats and responses, it will quickly lose its relevance and will not serve the purpose intended.

For the framework to serve the purpose of providing a common vocabulary for a skills map of cybersecurity for governments, academia and businesses in EU, it must stay in touch with new developments, incorporate them and stay responsive to the needs of its users. It is crucial that the process is well defined and transparent so that it can retain and augment credibility with stakeholders. On the other hand, it must have appropriate structures and processes which allow for uptake of the framework in the various fields of activities, adapting to the particular uses and specificities.

Major stakeholders of the Framework are identified as follows:

- Policymakers at EU and Member State level, who aim to understand the issues relating to cyber skills, emerging needs and target policy actions;
- Industry that operates in the cybersecurity field, as well as industry that needs to protect itself from cybersecurity threats;
- Academia, vocational training entities, all levels of education systems which train cybersecurity professionals and cybersecurity aware users;
- EU citizens, those who need to be aware of cyber threats and become safer users, as well as those planning for a career path in the cybersecurity field.

All diverse groups of stakeholders need to have a common language to assess the situation, plan for the future, self-organize and communicate between interested parties.

Thus, two essential governance processes are defined:

- Upstream – the process of updating the framework by collecting input from stakeholders and the wider public, which results in releasing new versions of the framework;
- Downstream – the process of coordinating dissemination and usage of the framework for specific activity areas, facilitating uptake and increasing relevance by usage.

6.4.1.1 Sparta Framework Governance bodies

We now turn to a discussion of the proposed structures and organizational bodies (groups) that will support Upstream and Downstream processes, and in turn ensure relevant and effective outcomes.

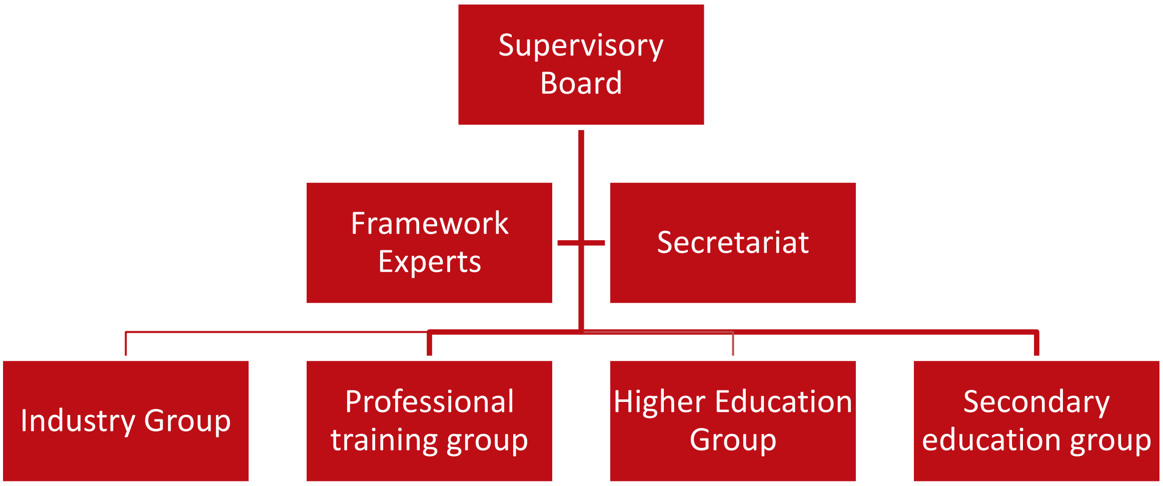


Figure 8: SPARTA Framework Governance bodies

The Secretariat serves as the technical body for servicing the needs of the Supervisory Board, Framework Experts and the remaining groups. It is responsible for providing technical tools, organizational administration, facilitation of public consultations, information dissemination etc.

Framework experts consist of highly competent cybersecurity experts selected to develop the Sparta Framework. They formulate wording, decide on removing and updating entries in the framework, and make final entries to the framework.

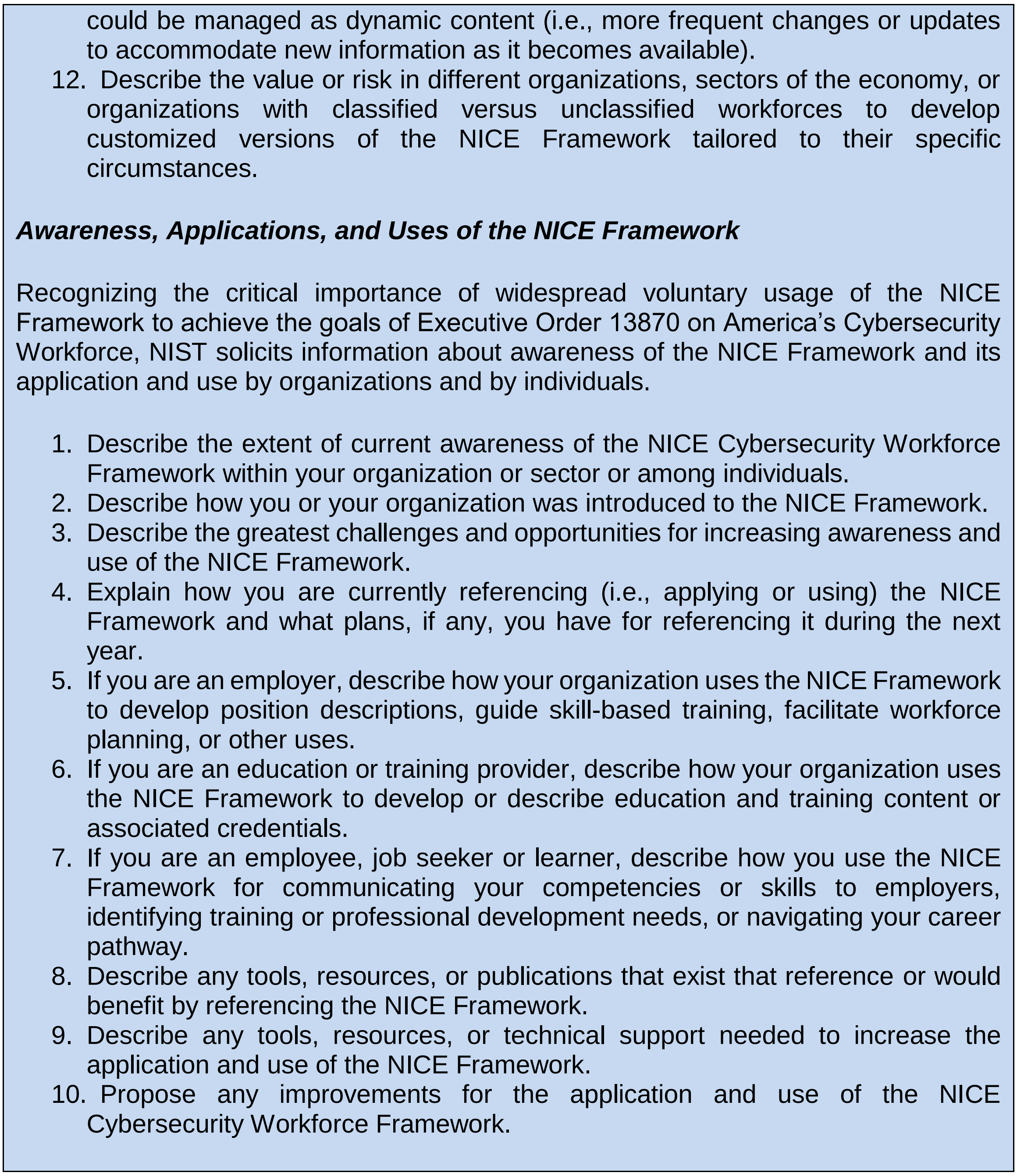
The Supervisory Board is responsible for maintaining the integrity of the governance processes and takes final responsibility for the health of the framework, its processes, including selection and appointment. The Supervisory Board should include representatives of academia, business and EC/MS's, to ensure that there are a sustainable collaboration effort and buy-in from the major stakeholders.

Various groups consist of area representatives who aim to leverage the use of the framework in relevant areas, discussing best practices of dissemination, education, and guidance.

Update of the framework process

Framework Experts will prepare the text for public distribution, with guiding questions and remarks, to facilitate input from the public.

> ***This is an example of the NIST NICE request for input communication*:**
>
> ***Improvements to the NICE Framework***
>
> The following topics are intended to help NIST and its partners who are part of the NICE Community to learn about experiences in applying and using the NICE Framework and explore opportunities for improvement.
>
> 1. Describe what components of the NICE Framework have been most useful to you and why.
> 2. Describe what components of the NICE Framework have been least useful to you and why.
> 3. Share any key concepts or topics that you believe are missing from the NICE Framework. Please explain what they are and why they merit special attention.
> 4. Describe how the NICE Framework can be more useful to a variety of audiences (i.e. employers, employees, education and training providers, learners, small enterprises, etc.).
> 5. Describe the potential benefits or challenges experienced when aligning the NICE Framework more closely with other related standards, guidance, or resources (e.g., NIST Framework for Critical Infrastructure Cybersecurity, NIST Privacy Framework, other NIST Special Publications, etc.).
> 6. Explain if you think the scope of the covered workforce, as stated by the NICE Framework needs to be adjusted.
> 7. Describe any improvements that might be made in the current organization of the NICE Framework and its major components such as Categories, Specialty Areas, Work Roles, Knowledge, Skills, Abilities, and Tasks.
> 8. Describe how the NICE Framework can best document and describe Knowledge, Skills, Ability, and Task statements as well as Competency Areas.
> 9. Explain whether the NICE Framework indicates which Knowledge, Skills, and Abilities could be considered as foundational for all workforces that regularly interact with networks, systems, and data in cyberspace.
> 10. For each NICE Framework work role, please provide an informative reference that you would like the NICE Framework Resource Center to reference.
> 11. Describe which components of the NICE Framework you think are best left as static content and would not change until the next revision and which components



could be managed as dynamic content (i.e., more frequent changes or updates to accommodate new information as it becomes available).

12. Describe the value or risk in different organizations, sectors of the economy, or organizations with classified versus unclassified workforces to develop customized versions of the NICE Framework tailored to their specific circumstances.

Awareness, Applications, and Uses of the NICE Framework

Recognizing the critical importance of widespread voluntary usage of the NICE Framework to achieve the goals of Executive Order 13870 on America's Cybersecurity Workforce, NIST solicits information about awareness of the NICE Framework and its application and use by organizations and by individuals.

1. Describe the extent of current awareness of the NICE Cybersecurity Workforce Framework within your organization or sector or among individuals.
2. Describe how you or your organization was introduced to the NICE Framework.
3. Describe the greatest challenges and opportunities for increasing awareness and use of the NICE Framework.
4. Explain how you are currently referencing (i.e., applying or using) the NICE Framework and what plans, if any, you have for referencing it during the next year.
5. If you are an employer, describe how your organization uses the NICE Framework to develop position descriptions, guide skill-based training, facilitate workforce planning, or other uses.
6. If you are an education or training provider, describe how your organization uses the NICE Framework to develop or describe education and training content or associated credentials.
7. If you are an employee, job seeker or learner, describe how you use the NICE Framework for communicating your competencies or skills to employers, identifying training or professional development needs, or navigating your career pathway.
8. Describe any tools, resources, or publications that exist that reference or would benefit by referencing the NICE Framework.
9. Describe any tools, resources, or technical support needed to increase the application and use of the NICE Framework.
10. Propose any improvements for the application and use of the NICE Cybersecurity Workforce Framework.

Figure 9: Example of NIST NICE request for input communication (Source: https://www.nist.gov)

The Secretariat will request input from stakeholders and interested public, and it will provide the necessary facilities, forms, and anything else necessary to collect the required input. Upon review, all inputs will be published online.

Framework experts will review the proposed inputs and prepare updates to the framework.

Updates will be discussed in the Groups and in meetings with the Supervisory Board, after which Framework Experts will be advised on introducing the necessary amendments. When the common ground is arrived at, the Framework Experts decide on the final version of the revised framework and issue instructions to publish it.

Dissemination process

Specific groups are established for the work focused on championing the use of the Framework in dedicated areas. The aim of groups would be established to integrate the framework in the planning and day to day activities of the specific areas. The Framework should become a common language, a tool for planning skills development and acquisition, etc.

Groups gather together in web conference mode once a month to discuss how best to apply, disseminate, use and increase the impact of the network. As well, groups can be instrumental in facilitating the gathering of feedback on the limitations of the framework, and serve as an input mechanism.

Relation to SPARTA programs

This framework has originated as a direct product of the SPARTA program, but it is not limited to serve SPARTA alone. Discussions with interested EU parties in academia, industry, professional services and governments revealed a strong need for this kind of EU cybersecurity skills taxonomy, which could provide a way to understand the situation better and develop targeted policies and practical actions.

Thus, while the framework is being developed by the SPARTA project, further down the road it should lose direct connection to SPARTA itself. After established governance structures are functional, the SPARTA project should further provide insights and suggestions for updating items of the framework, but those suggestions would be reviewed and incorporated into the framework via the due process of Framework governance. Thus, no special treatment or special process of further SPARTA inputs would be necessary.

6.4.2 SPARTA CS Framework Sustainability outlook

Ensuring the sustainability of such a Skills framework is an exercise which requires good planning and diligence.

Sustainability rests on the following pillars:

- The development towards a complete version and validation;
- Wide acceptance;
- Implementation and rollout;
- Ensuring sustained relevance by continuous updates and dissemination efforts.

These pillars are significantly intertwined and will have a strong influence in sustaining a network of framework users – the more widely it is accepted, the stronger and more relevant it becomes. Sustained relevance depends very much on acceptance, as it fuels the enthusiasm of participants and provides valuable input for updating the content of the framework, making it forward-looking rather than just a snapshot of a moment-in-time.

Learning from the NIST NICE Framework experience and observations of various efforts in the EU, we consider these further in addressing the challenges facing the question of sustainability.

6.4.2.1 Wide acceptance

The Framework governance group would organize events/competitions and an information dissemination campaign, building a body of highly usable material in order to increase awareness and increase uptake of the framework.

The Framework governance group will engage in continuous and open dialogue as to how to identify, recruit, develop knowledge, skills and abilities that reflect the key aspects of the SPARTA Framework. This must be established with various groups functioning on different levels.

International Level: if the SPARTA CS Framework is to be considered as a valuable and promising structure for EU wide skills management, it is necessary to recognize it at the EU level and include as a reference in all relevant documents, recommendations, and projects.

Stakeholder Level:

- **Science and education** (Universities, colleges): we must ensure commitment from leading Universities offering cybersecurity programs and courses to accept and champion the taxonomy for its use. This should create momentum and attract other followers and adopters from academia.
- **Industry**: an industrial association's framework group will be set up to select companies that will champion use of the framework for their skills management processes and serve as examples of uptake, as well as providing observations and suggestions for improving the Framework. Industry and SME associations such as the European Digital SME Alliance and ECSO will get a broader insight on the challenges and lessons learned in this emerging field.
- **Professional Services**: Knowledge foundations, communities of practice maintaining ICT frameworks and standards, education and training programs designers, certification providers, all will be enlisted for purposes of adopting and supporting the Framework.

Member State Level: acceptance at the EU level would play a very important role, thus it is important that in relevant formats MS's would adopt the Framework for universal use.

Currently, many countries are working to develop their own unique standards and requirements which may make interoperability at the international level a more challenging and sometimes onerous process. Therefore, the following actions have to be taken into account to foster Framework roll out on the MS level:

- Continuous Adjustment of SPARTA cyber skills framework to MS specific challenges/items/task roles and priorities
- Identify additional areas of alignment between the Cybersecurity Skills Framework and existing and emerging MS frameworks
- Governance strategy - Identify an organization that would take on a leading role and responsibility of maintaining and supporting the framework at the MS level
- Define Approaches to using the CS Framework within MS Agencies
- Identify and share lessons learned from the use of the Framework by MS agencies
- Identify international collaboration opportunities and alignment possibilities of the framework with EU MS national priorities.

6.4.2.2 Implementation & rollout

Attracting key brains

An important part of this aspect will be to attract highly competent EU cybersecurity professionals to take part in the Framework Experts panel, and to take ownership of the framework and together develop creative and innovative ideas to increase cybersecurity capability in the EU.

Building and financing sustainable governance organization

To enable constructive discussion between industry, public sector and academia on the current status of cybersecurity skills issues, future development and measures to fill the skills gap, and strong leadership and long-term vision are necessary, with political-backing and a carefully planned implementation. Thus, Framework success will largely depend on establishing a reputable and efficient organization. It is important from the beginning to envision the organization which will serve the Framework.

A few organizations that could take a leading role in promoting the SPARTA Skills Framework might be considered:

- SPARTA Joint Centre of Competence Infrastructure (JCCI)
- European Cyber Security Organization (ECSO)
- Joint Research Centre (JRC)
- European Cybersecurity Industrial, Technology and Research Competence Center (this organization is still to be established).
- A new organization designated for the management of EU cybersecurity skills.

Feedback from the discussions with ECSO and JRC Europe demonstrated that all organizations are ready to support and make an active contribution towards establishing an EU cybersecurity skills management standard.

Financing must be ensured for the years to come, as this is an effort which will not lose importance in the foreseeable future.

6.4.2.3 Ensuring sustained relevance by continuous updates and dissemination efforts

The process of upstream updates and downstream dissemination is described in the earlier section on Update of the framework process. This process will ensure that the framework is constantly updated with the realities of the market and inputs from academia.

Recent research has identified that in areas of automation, data analytics, and complex threat intelligence, key cybersecurity technical skills will be required in the future. To interpret, learn and process security intelligence designed by and for humans requires a wide range of skills and competencies that include not only traditional technical skills but also the consideration of the social aspects of human behaviour influenced by new technologies and events. It is extremely important that further development of the cyber skills framework has to consider the relevance of integration of classical cyber security skills with new scientific disciplines enriched by the results of research programs, exercises and practical experience of defence and security practitioners.

Synergies and complementariness with EU initiatives and projects

Four projects financed by EC, namely SPARTA, CONCORDIA, ECHO, CyberSec4Europe are leading the development of cyber security approaches in different domains and sectors. Today all the pilots demonstrate great achievements and unique knowledge in cyber skills management. Established links and continued interaction with pilot projects will help to build synergies between the projects and foster progress towards implementation of the cyber security skills framework throughout EU.

Synergies with SPARTA research programs

The essence of the SPARTA project involves four programs (T-Shark, SAFAIR, HAII-T, and CAPE) with a clearly defined research mission to develop cyber capacities and supply EU industry with new methods, new approaches and new technical means to ensure its cyber security. SPARTA research topics have been selected from the list of unresolved issues and it focuses on the emerging future challenges:

- Comprehensive threat intelligence based on cognitive computer capabilities aimed at supporting and protecting decision-making processes (T-Shark)
- Self-healing and adaptive security that continuously adapts countermeasures to mitigate risks and ensure continuous trust in sovereign and foreign-sourced components, systems, and services (CAPE)
- Development of a secure-by-design Intelligent Infrastructure foundation aimed at leapfrogging incumbents and positioning European industry to be at the forefront of the upcoming II race (HAII-T)
- Investigation of approaches that make systems using AI more reliable and resilient through a better understanding of the threat landscape; providing methods and tools for analysis of security threats for AI systems. (SAFAIR)

Significantly, during SPARTA implementation four research programs will be transferred to centres of expertise supplemented by virtual teams of researchers and supported by the SPARTA Joint Centre of Competence Infrastructure (JCCI).

Over the long term, JCCI will play a leading role ensuring that in-depth knowledge gained through numerous research and practical exercises of SPARTA programmes will be continuously transferred to industry, EU central agencies and reflected in the professional training and education programmes. In addition, JCCI on behalf of the SPARTA community will take an active role in the governance and implementation of the cyber skills framework to ensure that CS framework meets operational, sustainable and continuously improving requirements and evolving industry needs.

Dissemination

- As discussed in the chapter on Framework Governance, dissemination groups should be established over the longer term to make the SPARTA Framework a truly universal EU language of cybersecurity skills. Groups will continuously discuss the best ways to ensure that the Framework is used and delivers as promised.
- SPARTA Framework leadership will work on engaging third parties to apply the framework for a variety of applications, including such examples as targeting Universities for specific skills education, providing career guidance for professionals and students in cybersecurity adjacent fields, competitions, awareness events, etc.
- Dissemination efforts will leverage established networks with the initiatives of EC and the Member States. Several countries such as Italy and Spain have already built networks connecting almost all the main national actors; France and Germany operate regional and local excellence centres and are strongly involved in the consolidation of their national ecosystems. This process is envisaged in several other Member States. Cooperation among research/academia, industry, government and ethical hacking organizations is recognized to be the main ingredient in support of a healthy national research network in so relevant field as cybersecurity.

6.4.3 Open questions for further discussions

6.4.3.1 Relationship with NICE Framework

One of the key sources of the first version of the SPARTA Framework was the NIST NICE Framework that was amended with EU specific items and future-looking SPARTA inputs.

NIST in the USA is a standards organization supporting the NICE Framework. This means that NICE is being updated from time to time, by modifying existing entries, subtracting and amending as called for. Thus, it is necessary to discuss how an EU focused framework will be developed and sustained.

OPTION 1. SPARTA Framework makes a “fork” – takes the NICE Framework into account at the current stage and amends it to adapt to EU realities and introduces other necessary amendments and/or changes. Further on, the SPARTA Framework would be maintained and updated independently from the NICE Framework. Over time, it is natural to expect that gaps between frameworks will grow larger and become less comparable.

OPTION 2. SPARTA Framework would produce amendments to the NICE Framework defining tasks - roles - KSA’s in line with the NICE Framework itself. These amendments and changes would be incorporated very attentively with the aim of keeping the NICE Framework intact, while clearly identifying EU specific items in the framework with designated numbering schemes, etc.

With this latter option, when the NICE Framework issues updates, such updates would be automatically propagated for use in the SPARTA Framework. After every update by NICE, the SPARTA Framework would review EU specific items and update them accordingly.

In this way, the EU would essentially continue using the NICE Framework as updated by the NIST organization and would follow its development path. The SPARTA Framework governance body would be triggered by NICE updates and would be responsible only for the small task of identifying and maintaining EU specific task-roles-KSA’s as addenda to the framework.

6.4.3.2 Involving Member States in the governance of the Framework

For the Framework to achieve the purpose of becoming a truly common taxonomy for EU wide cybersecurity skills classification, Member States have to be fully involved and feel that they have a relevant stake in the Framework.

On the other hand, with few resources, it is impossible to employ a comprehensive coordination/consultation process with all Member States due to their sheer numbers, thus expanding the Supervisory Board with representatives from all MS's does not seem like an option.

Further discussion is needed to determine solutions and appropriate governance structures to involve all MS's in aligning their interests, while not risking overinflating the structure and losing efficiency.

6.4.3.3 Ownership of the Framework

As discussed in the Governance sections, an organization that will be mandated with the onerous task of sustaining the Framework is one of the key pillars of success, perhaps even the single most important one.

Organizations that might be capable of extending their mandates to support governance of the Framework include, but are not limited to:

- SPARTA Joint Centre of Competence Infrastructure (JCCI)
- European Cyber Security Organization (ECSO)
- Joint Research Centre (JRC)
- European Cybersecurity Industrial, Technology and Research Competence Center (this organization is yet to be established).
- A new organization designated for the management of EU cybersecurity skills.

On the other hand, the establishment of a new organization is also an option.

Financing must be ensured for the years to come, as this CS effort will not lose its importance in the foreseeable future.

Further discussions are in order to identify potential organizations, possible alignment with the SPARTA Framework, as well as its aims, reputation and financing.

Chapter 7 Conclusion

This document attempts to analyse the state of knowledge regarding skills management, by reviewing best practices and proposing a viable way forward with the development of an EU based cybersecurity skills framework.

This document serves as a basis for setting in motion a process of development of a comprehensive European cybersecurity skills framework that will result in a more complete and vigorous workforce. It should be implemented concurrently with a governance structure that would allow for being continuously updated and serve as a platform for meeting the needs of various market actors who deal regularly with the supply and demand sides of cybersecurity skills. We have focused especially on the feasibility of such an approach and the possibility of building on the results of work already undertaken internationally and in the EU. Significantly, readers and evaluators of this document should consider that there was no intent to produce a point-in-time snapshot of a skills matrix, which would rapidly lose its validity due to the fast pace of change in the cybersecurity field.

Consider our basic assumption: a comprehensive "Cybersecurity Skills Framework" must unequivocally include the principal components of roles and corresponding knowledge/skills required to fulfil these roles; and these should be defined and mapped accordingly, providing a full picture of the framework.

In developing such a framework an exhaustive classification of roles, functions, actual tasks, and the complete scope of work performed in daily activities are of critical importance. The European documents that we analysed did not describe these elements in full, only partially. However, only by examining activities, described by tasks, can one arrive at a full understanding of the skills required to perform those tasks. In any case, we determined that the best example of a framework that attempted to conceptualize all aspects of ICT skills, including roles and activities within the scope of cybersecurity, was the US-based National Initiative for Cybersecurity Education (NICE) because it categorized Knowledge, Skills, and Abilities by means of fine details and described their respective features in the most practical and powerful way, which would allow the framework to be leveraged further.

Analysis of current initiatives indicated that the NICE Framework, coupled with JRC Cybersecurity domains taxonomy, represent the most reasonable starting point, providing a comprehensive and accommodative structure for incorporating EU specific realities into an emerging skills landscape.

What is more, we have outlined how the NICE Framework has been taken up as a reference point for the development and validation of the SPARTA CS Framework, which has focused on three key aspects:

- Inclusivity – embedding EU specific legislation of relevance into the Framework;
- Applicability - testing whether the Framework provides value for academia by i) facilitating analysis of existing curricula, ii) guiding efforts for the enrichment of curricula in relation to necessary skills, and iii) helping industry to analyse actual roles and skillsets within the organization;
- Adaptability – the ability of the Framework to include and provide a clear indication of emerging roles and skills, required for cybersecurity operations in the near future.

These development and validation activities confirmed that the NICE Framework could be adapted and developed further into a viable SPARTA CS Framework.

Our experience in examining the NICE Framework and observations of various efforts in the EU, led us to consider the question of sustainability as a key aspect in developing an EU wide CS Skills Framework. Hence, significant attention was placed on this aspect, which included the following elements:

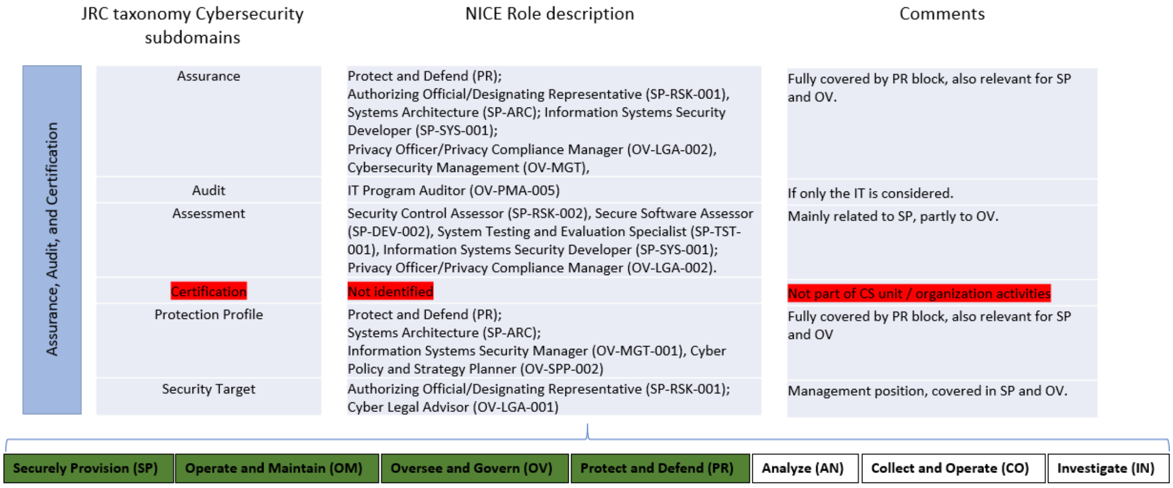
- Development of a complete validated version;

- Wide acceptance;
- Implementation and rollout;
- Ensuring sustained relevance by means of continuous updates and a sound dissemination strategy.

These elements are significantly intertwined and will have a strong influence in sustaining a network of framework users – the wider the acceptance, the stronger and more relevant it becomes. Sustained relevance depends very much on acceptance, as it fuels the enthusiasm of participants and provides valuable input for updating the content of the framework, making it forward-looking rather than just a snapshot of a moment-in-time.

Annex 1 Mapping of JRC taxonomy and NICE Framework

JRC dimension: Assurance, Audit and Certification



Assurance, Audit, and Certification

JRC taxonomy Cybersecurity subdomains	NICE Role description	Comments

Assurance	Protect and Defend (PR);
	Authorizing Official/Designating Representative (SP-RSK-001), Systems Architecture (SP-ARC); Information Systems Security Developer (SP-SYS-001);
	Privacy Officer/Privacy Compliance Manager (OV-LGA-002), Cybersecurity Management (OV-MGT),
		Fully covered by PR block, also relevant for SP and OV.

Audit	IT Program Auditor (OV-PMA-005)	If only the IT is considered.
Assessment	Security Control Assessor (SP-RSK-002), Secure Software Assessor (SP-DEV-002), System Testing and Evaluation Specialist (SP-TST-001), Information Systems Security Developer (SP-SYS-001); Privacy Officer/Privacy Compliance Manager (OV-LGA-002).	Mainly related to SP, partly to OV.
Certification	Not identified	Not part of CS unit / organization activities

Protection Profile	Protect and Defend (PR);
	Systems Architecture (SP-ARC);
	Information Systems Security Manager (OV-MGT-001), Cyber Policy and Strategy Planner (OV-SPP-002)
		Fully covered by PR block, also relevant for SP and OV

Security Target	Authorizing Official/Designating Representative (SP-RSK-001); Cyber Legal Advisor (OV-LGA-001)	Management position, covered in SP and OV.

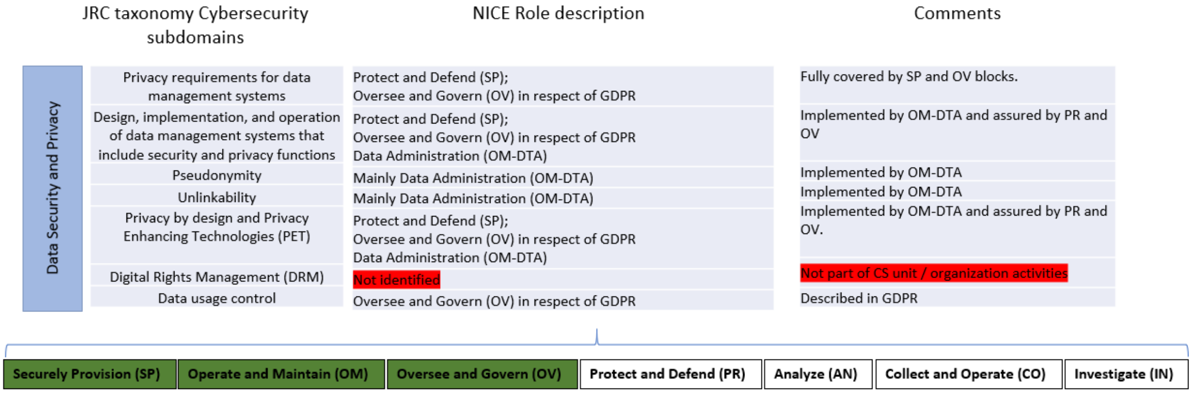
Securely Provision (SP) | Operate and Maintain (OM) | Oversee and Govern (OV) | Protect and Defend (PR) | Analyze (AN) | Collect and Operate (CO) | Investigate (IN)

Figure 10: JRC dimension: Assurance, Audit and Certification

Input questions and comments

- Please provide any relevant comments on the mapping, if any.
- Are certification activities performed by CS organizational unit or national CS institutions (not specific for Certification)?
- Is assurance mainly the responsibility of the Secure Provision (SP) and Oversee and Govern (OV) Role blocks?

JRC dimension: Data Security and Privacy



Data Security and Privacy

JRC taxonomy Cybersecurity subdomains	NICE Role description	Comments
Privacy requirements for data management systems	Protect and Defend (SP); Oversee and Govern (OV) in respect of GDPR	Fully covered by SP and OV blocks.
Design, implementation, and operation of data management systems that include security and privacy functions	Protect and Defend (SP); Oversee and Govern (OV) in respect of GDPR Data Administration (OM-DTA)	Implemented by OM-DTA and assured by PR and OV
Pseudonymity	Mainly Data Administration (OM-DTA)	Implemented by OM-DTA
Unlinkability	Mainly Data Administration (OM-DTA)	Implemented by OM-DTA
Privacy by design and Privacy Enhancing Technologies (PET)	Protect and Defend (SP); Oversee and Govern (OV) in respect of GDPR Data Administration (OM-DTA)	Implemented by OM-DTA and assured by PR and OV.
Digital Rights Management (DRM)	Not identified	Not part of CS unit / organization activities
Data usage control	Oversee and Govern (OV) in respect of GDPR	Described in GDPR

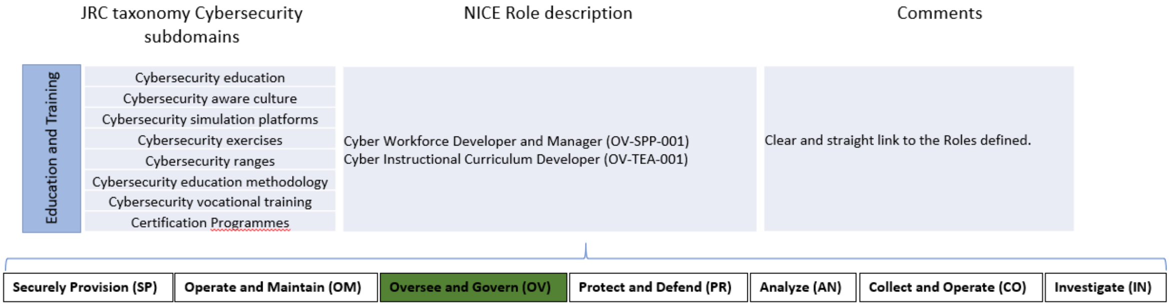
Securely Provision (SP) | Operate and Maintain (OM) | Oversee and Govern (OV) | Protect and Defend (PR) | Analyze (AN) | Collect and Operate (CO) | Investigate (IN)

Figure 11: RC dimension: Data Security and Privacy

Input questions and comments

- Please provide any relevant comments on the mapping, if any.
- Should Digital Rights Management (DRM) be considered in the scope of activities performed by CS organizational unit or national CS institutions?

JRC: Education and Training



	JRC taxonomy Cybersecurity subdomains	NICE Role description	Comments
Education and Training	Cybersecurity education Cybersecurity aware culture Cybersecurity simulation platforms Cybersecurity exercises Cybersecurity ranges Cybersecurity education methodology Cybersecurity vocational training Certification Programmes	Cyber Workforce Developer and Manager (OV-SPP-001) Cyber Instructional Curriculum Developer (OV-TEA-001)	Clear and straight link to the Roles defined.

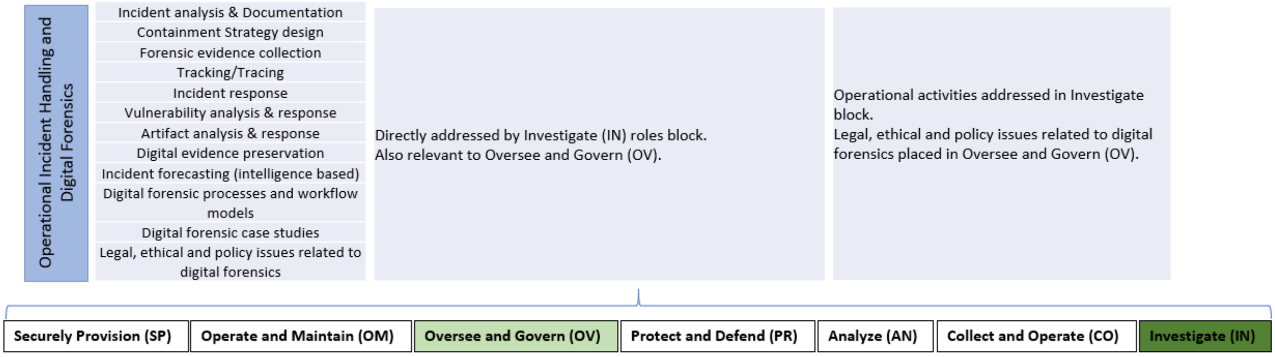
Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)	Investigate (IN)

Figure 12: JRC: Education and Training

Input questions and comments

- Please provide any relevant comments on the mapping, if any.

JRC dimension: Operational Incident Handling and Digital Forensics



Operational Incident Handling and Digital Forensics	Incident analysis & Documentation Containment Strategy design Forensic evidence collection Tracking/Tracing Incident response Vulnerability analysis & response Artifact analysis & response Digital evidence preservation Incident forecasting (intelligence based) Digital forensic processes and workflow models Digital forensic case studies Legal, ethical and policy issues related to digital forensics	Directly addressed by Investigate (IN) roles block. Also relevant to Oversee and Govern (OV).	Operational activities addressed in Investigate block. Legal, ethical and policy issues related to digital forensics placed in Oversee and Govern (OV).

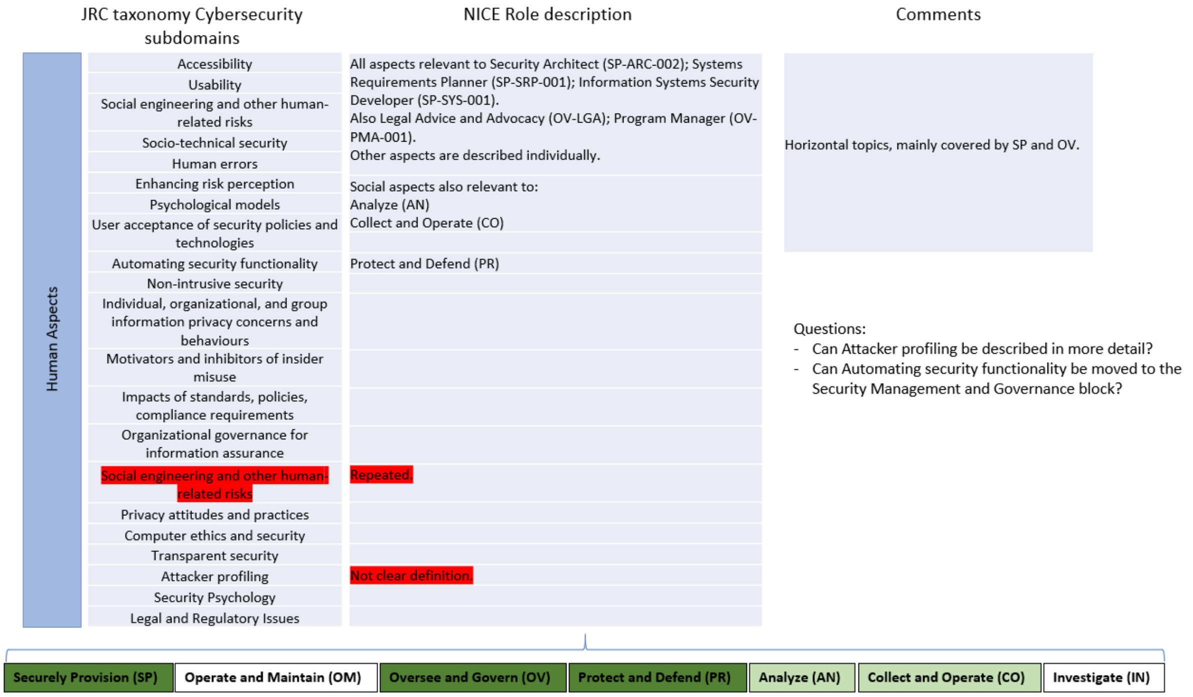
Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)	Investigate (IN)

Figure 13: JRC dimension: Operational Incident Handling and Digital Forensics

Input questions and comments

- Please provide any relevant comments on the mapping, if any.

JRC dimension: Human Aspects



	JRC taxonomy Cybersecurity subdomains	NICE Role description	Comments
Human Aspects	Accessibility	All aspects relevant to Security Architect (SP-ARC-002); Systems Requirements Planner (SP-SRP-001); Information Systems Security Developer (SP-SYS-001). Also Legal Advice and Advocacy (OV-LGA); Program Manager (OV-PMA-001). Other aspects are described individually.	Horizontal topics, mainly covered by SP and OV.
	Usability		
	Social engineering and other human-related risks		
	Socio-technical security		
	Human errors		
	Enhancing risk perception	Social aspects also relevant to: Analyze (AN) Collect and Operate (CO)	
	Psychological models		
	User acceptance of security policies and technologies		
	Automating security functionality	Protect and Defend (PR)	
	Non-intrusive security		
	Individual, organizational, and group information privacy concerns and behaviours		Questions: - Can Attacker profiling be described in more detail? - Can Automating security functionality be moved to the Security Management and Governance block?
	Motivators and inhibitors of insider misuse		
	Impacts of standards, policies, compliance requirements		
	Organizational governance for information assurance		
	Social engineering and other human-related risks	Repeated.	
	Privacy attitudes and practices		
	Computer ethics and security		
	Transparent security		
	Attacker profiling	Not clear definition.	
	Security Psychology		
	Legal and Regulatory Issues		

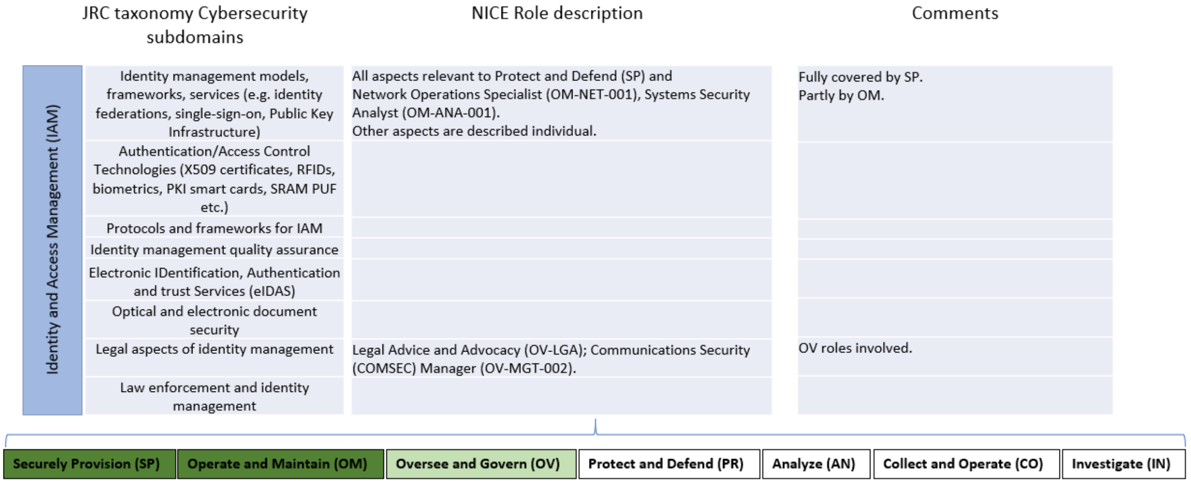
Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)	Investigate (IN)

Figure 14: JRC dimension: Human Aspects

Input questions and comments

- Please provide any relevant comments on the mapping, if any.

JRC dimension: Identity and Access Management



	JRC taxonomy Cybersecurity subdomains	NICE Role description	Comments
Identity and Access Management (IAM)	Identity management models, frameworks, services (e.g. identity federations, single-sign-on, Public Key Infrastructure)	All aspects relevant to Protect and Defend (SP) and Network Operations Specialist (OM-NET-001), Systems Security Analyst (OM-ANA-001). Other aspects are described individual.	Fully covered by SP. Partly by OM.
	Authentication/Access Control Technologies (X509 certificates, RFIDs, biometrics, PKI smart cards, SRAM PUF etc.)		
	Protocols and frameworks for IAM		
	Identity management quality assurance		
	Electronic IDentification, Authentication and trust Services (eIDAS)		
	Optical and electronic document security		
	Legal aspects of identity management	Legal Advice and Advocacy (OV-LGA); Communications Security (COMSEC) Manager (OV-MGT-002).	OV roles involved.
	Law enforcement and identity management		

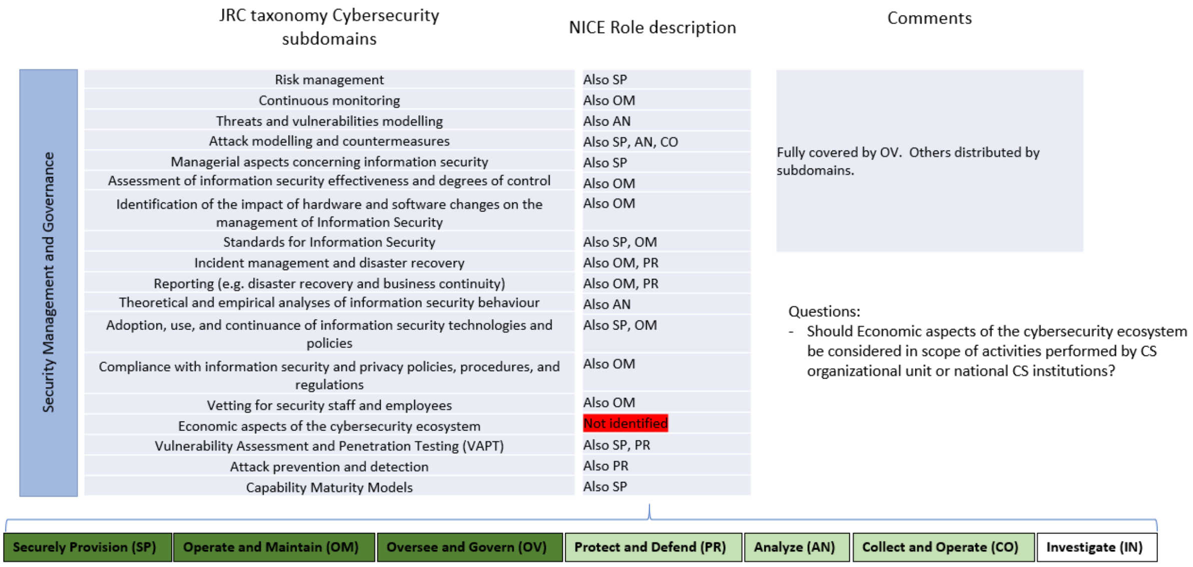
Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)	Investigate (IN)

Figure 15: JRC dimension: Identity and Access Management

Input questions and comments

- Please provide any relevant comments on the mapping, if any.
- Should Identity and Access Management (IAM) be part of the Applications and Technologies dimension?

JRC dimension: Security Management and Governance



	JRC taxonomy Cybersecurity subdomains	NICE Role description	Comments
Security Management and Governance	Risk management	Also SP	Fully covered by OV. Others distributed by subdomains.
	Continuous monitoring	Also OM	
	Threats and vulnerabilities modelling	Also AN	
	Attack modelling and countermeasures	Also SP, AN, CO	
	Managerial aspects concerning information security	Also SP	
	Assessment of information security effectiveness and degrees of control	Also OM	
	Identification of the impact of hardware and software changes on the management of Information Security	Also OM	
	Standards for Information Security	Also SP, OM	
	Incident management and disaster recovery	Also OM, PR	
	Reporting (e.g. disaster recovery and business continuity)	Also OM, PR	
	Theoretical and empirical analyses of information security behaviour	Also AN	Questions: - Should Economic aspects of the cybersecurity ecosystem be considered in scope of activities performed by CS organizational unit or national CS institutions?
	Adoption, use, and continuance of information security technologies and policies	Also SP, OM	
	Compliance with information security and privacy policies, procedures, and regulations	Also OM	
	Vetting for security staff and employees	Also OM	
	Economic aspects of the cybersecurity ecosystem	Not identified	
	Vulnerability Assessment and Penetration Testing (VAPT)	Also SP, PR	
	Attack prevention and detection	Also PR	
	Capability Maturity Models	Also SP	

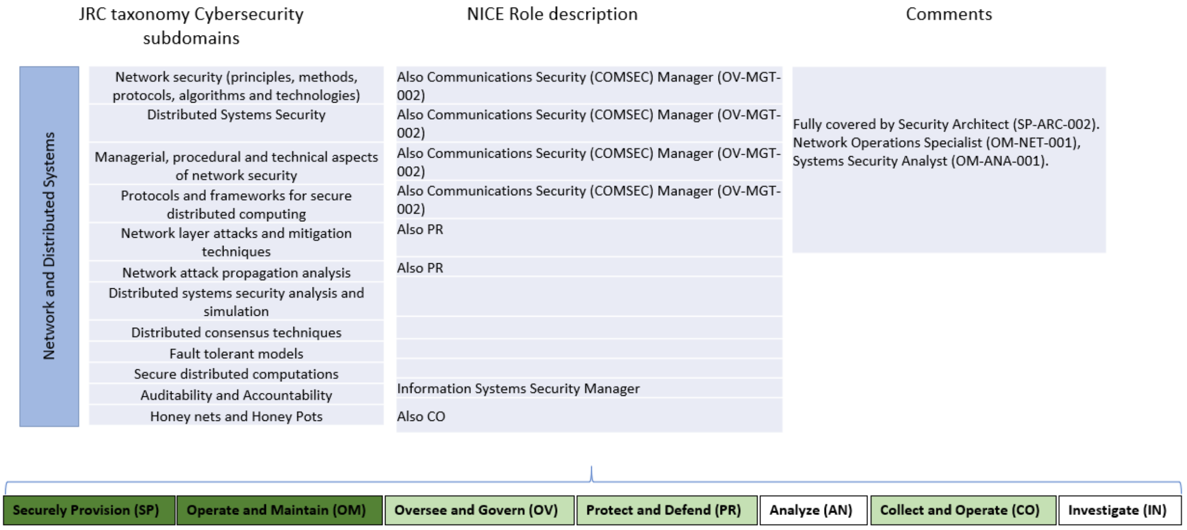
Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)	Investigate (IN)

Figure 16: JRC dimension: Security Management and Governance

Input questions and comments

- Please provide any relevant comments on the mapping, if any.

JRC dimension: Network and Distributed Systems



	JRC taxonomy Cybersecurity subdomains	NICE Role description	Comments
Network and Distributed Systems	Network security (principles, methods, protocols, algorithms and technologies)	Also Communications Security (COMSEC) Manager (OV-MGT-002)	Fully covered by Security Architect (SP-ARC-002). Network Operations Specialist (OM-NET-001), Systems Security Analyst (OM-ANA-001).
	Distributed Systems Security	Also Communications Security (COMSEC) Manager (OV-MGT-002)	
	Managerial, procedural and technical aspects of network security	Also Communications Security (COMSEC) Manager (OV-MGT-002)	
	Protocols and frameworks for secure distributed computing	Also Communications Security (COMSEC) Manager (OV-MGT-002)	
	Network layer attacks and mitigation techniques	Also PR	
	Network attack propagation analysis	Also PR	
	Distributed systems security analysis and simulation		
	Distributed consensus techniques		
	Fault tolerant models		
	Secure distributed computations		
	Auditability and Accountability	Information Systems Security Manager	
	Honey nets and Honey Pots	Also CO	

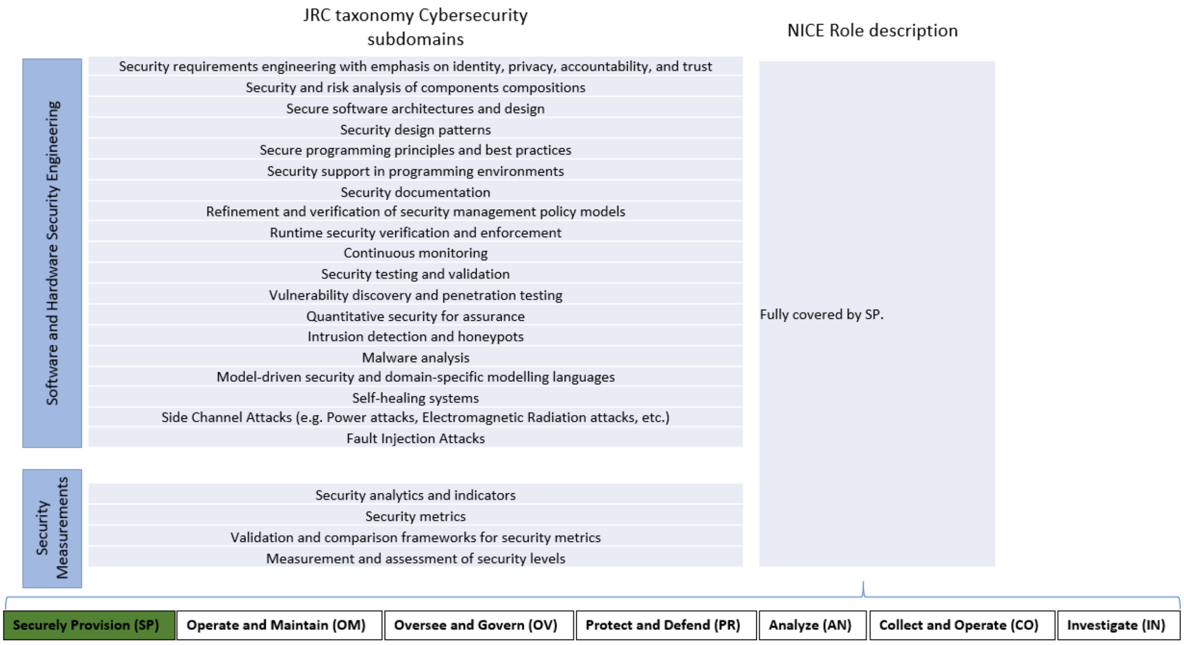
Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)	Investigate (IN)

Figure 17: JRC dimension: Network and Distributed Systems

Input questions and comments

- Please provide any relevant comments on the mapping, if any.

JRC dimension: Software and Hardware Security Engineering and JRC dimension: Security Measurements



JRC taxonomy Cybersecurity subdomains

NICE Role description

Software and Hardware Security Engineering

- Security requirements engineering with emphasis on identity, privacy, accountability, and trust
- Security and risk analysis of components compositions
- Secure software architectures and design
- Security design patterns
- Secure programming principles and best practices
- Security support in programming environments
- Security documentation
- Refinement and verification of security management policy models
- Runtime security verification and enforcement
- Continuous monitoring
- Security testing and validation
- Vulnerability discovery and penetration testing
- Quantitative security for assurance
- Intrusion detection and honeypots
- Malware analysis
- Model-driven security and domain-specific modelling languages
- Self-healing systems
- Side Channel Attacks (e.g. Power attacks, Electromagnetic Radiation attacks, etc.)
- Fault Injection Attacks

Security Measurements

- Security analytics and indicators
- Security metrics
- Validation and comparison frameworks for security metrics
- Measurement and assessment of security levels

Fully covered by SP.

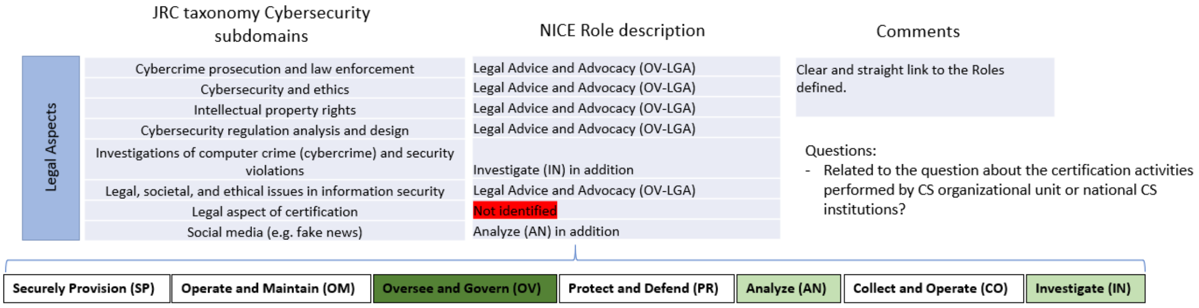
Securely Provision (SP) | Operate and Maintain (OM) | Oversee and Govern (OV) | Protect and Defend (PR) | Analyze (AN) | Collect and Operate (CO) | Investigate (IN)

Figure 18: JRC dimension: Security Measurements

Input questions and comments

- Please provide any relevant comments on the mapping, if any.

JRC dimension: Legal Aspects



Legal Aspects

JRC taxonomy Cybersecurity subdomains	NICE Role description
Cybercrime prosecution and law enforcement	Legal Advice and Advocacy (OV-LGA)
Cybersecurity and ethics	Legal Advice and Advocacy (OV-LGA)
Intellectual property rights	Legal Advice and Advocacy (OV-LGA)
Cybersecurity regulation analysis and design	Legal Advice and Advocacy (OV-LGA)
Investigations of computer crime (cybercrime) and security violations	Investigate (IN) in addition
Legal, societal, and ethical issues in information security	Legal Advice and Advocacy (OV-LGA)
Legal aspect of certification	Not identified
Social media (e.g. fake news)	Analyze (AN) in addition

Comments

Clear and straight link to the Roles defined.

Questions:
- Related to the question about the certification activities performed by CS organizational unit or national CS institutions?

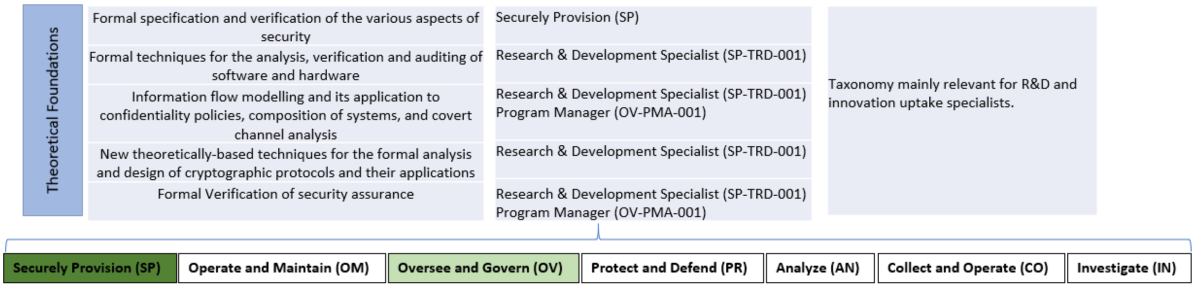
Securely Provision (SP) | Operate and Maintain (OM) | Oversee and Govern (OV) | Protect and Defend (PR) | Analyze (AN) | Collect and Operate (CO) | Investigate (IN)

Figure 19: JRC dimension: Legal Aspects

Input questions and comments

- Please provide any relevant comments on the mapping, if any.

JRC dimension: Theoretical Foundations



Theoretical Foundations	Formal specification and verification of the various aspects of security	Securely Provision (SP)	Taxonomy mainly relevant for R&D and innovation uptake specialists.
	Formal techniques for the analysis, verification and auditing of software and hardware	Research & Development Specialist (SP-TRD-001)	
	Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis	Research & Development Specialist (SP-TRD-001) Program Manager (OV-PMA-001)	
	New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications	Research & Development Specialist (SP-TRD-001)	
	Formal Verification of security assurance	Research & Development Specialist (SP-TRD-001) Program Manager (OV-PMA-001)	

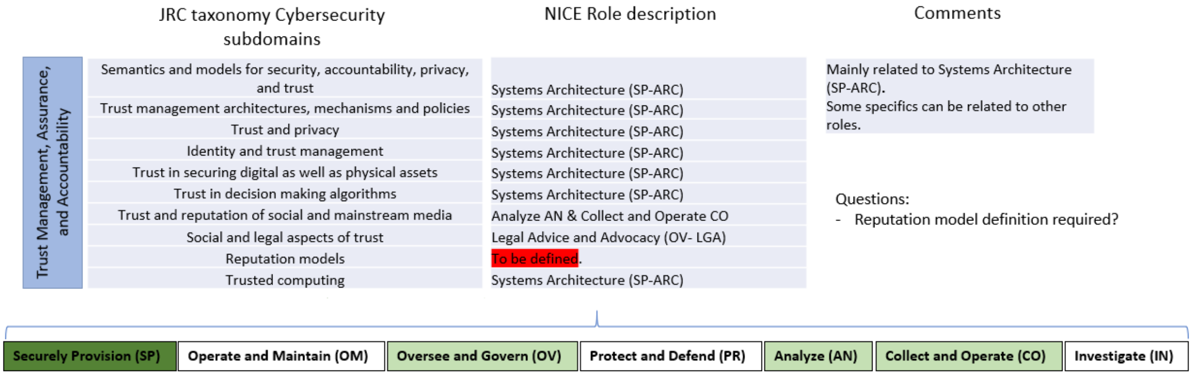
Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)	Investigate (IN)

Figure 20: JRC dimension: Theoretical Foundations

Input questions and comments

- Please provide any relevant comments on the mapping, if any.

JRC dimension: Trust Management, Assurance, and Accountability



	JRC taxonomy Cybersecurity subdomains	NICE Role description	Comments
Trust Management, Assurance, and Accountability	Semantics and models for security, accountability, privacy, and trust	Systems Architecture (SP-ARC)	Mainly related to Systems Architecture (SP-ARC). Some specifics can be related to other roles.
	Trust management architectures, mechanisms and policies	Systems Architecture (SP-ARC)	
	Trust and privacy	Systems Architecture (SP-ARC)	
	Identity and trust management	Systems Architecture (SP-ARC)	
	Trust in securing digital as well as physical assets	Systems Architecture (SP-ARC)	
	Trust in decision making algorithms	Systems Architecture (SP-ARC)	Questions: - Reputation model definition required?
	Trust and reputation of social and mainstream media	Analyze AN & Collect and Operate CO	
	Social and legal aspects of trust	Legal Advice and Advocacy (OV- LGA)	
	Reputation models	To be defined.	
	Trusted computing	Systems Architecture (SP-ARC)	

Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)	Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)	Investigate (IN)

Figure 21: JRC dimension: Trust Management, Assurance, and Accountability

Input questions and comments

- Please provide any relevant comments on the mapping, if any.

Annex 2 Task list of NICE Privacy Officer/Privacy Compliance Manager role

Oversee and Govern (OV) Legal Advice and Advocacy (LGA)	**Privacy Officer/Privacy Compliance Manager (OV-LGA-002)**: Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
Task ID	**Task**
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.
T0029	Conduct functional and connectivity testing to ensure continuing operability.
T0930	Establish a risk management strategy for the organization that includes a determination of risk tolerance.
T0032	Conduct Privacy Impact Assessments (PIAs) of the application’s security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).
T0066	Develop and maintain strategic plans.
T0098	Evaluate contracts to ensure compliance with funding, legal, and program requirements.
T0099	Evaluate cost/benefit, economic, and risk analysis in decision-making process.
T0131	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.
T0133	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s cybersecurity program.
T0188	Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions.
T0381	Present technical information to technical and nontechnical audiences.
T0384	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.
T0478	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.
T0861	Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations.
T0862	Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.
T0863	Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.
T0864	Liaise with regulatory and accrediting bodies.

Oversee and Govern (OV) **Legal Advice and Advocacy (LGA)**	**Privacy Officer/Privacy Compliance Manager (OV-LGA-002)**: Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
Task ID	**Task**
T0865	Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.
T0866	Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
T0867	Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.
T0868	Work with business teams and senior management to ensure awareness of "best practices" on privacy and data security issues.
T0869	Work with organization senior management to establish an organization-wide Privacy Oversight Committee
T0870	Serve in a leadership role for Privacy Oversight Committee activities
T0871	Collaborate on cyber privacy and security policies and procedures
T0872	Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation
T0873	Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations
T0874	Provide strategic guidance to corporate officers regarding information resources and technology
T0875	Assist the Security Officer with the development and implementation of an information infrastructure
T0876	Coordinate with the Corporate Compliance Officer regarding procedures for documenting and reporting self-disclosures of any evidence of privacy violations.
T0877	Work cooperatively with applicable organization units in overseeing consumer information access rights
T0878	Serve as the information privacy liaison for users of technology systems
T0879	Act as a liaison to the information systems department
T0880	Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations
T0881	Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties
T0882	Conduct on-going privacy training and awareness activities
T0883	Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security
T0884	Work with organization administration, legal counsel and other related parties to represent the organization's information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard.

Oversee and Govern (OV) Legal Advice and Advocacy (LGA)	**Privacy Officer/Privacy Compliance Manager (OV-LGA-002)**: Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
Task ID	**Task**
T0885	Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee
T0886	Work with External Affairs to respond to press and other inquiries regarding concern over consumer and employee data
T0887	Provide leadership for the organization’s privacy program
T0888	Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization
T0889	Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization’s workforce, extended workforce and for all business associates in cooperation with Human Resources, the information security officer, administration and legal counsel as applicable
T0890	Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures
T0891	Resolve allegations of noncompliance with the corporate privacy policies or notice of information practices
T0892	Develop and coordinate a risk management and compliance framework for privacy
T0893	Undertake a comprehensive review of the company’s data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies.
T0894	Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations
T0895	Establish a process for receiving, documenting, tracking, investigating and acting on all complaints concerning the organization’s privacy policies and procedures
T0896	Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity
T0897	Provide leadership in the planning, design and evaluation of privacy and security related projects
T0898	Establish an internal privacy audit program
T0899	Periodically revise the privacy program considering changes in laws, regulatory or company policy
T0900	Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel
T0901	Assure that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information
T0902	Monitor systems development and operations for security and privacy compliance

Oversee and Govern (OV) Legal Advice and Advocacy (LGA)	**Privacy Officer/Privacy Compliance Manager (OV-LGA-002)**: Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.
Task ID	**Task**
T0903	Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected
T0904	Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions
T0905	Review all system-related information security plans to ensure alignment between security and privacy practices
T0906	Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization's policies, procedures and legal requirements
T0907	Account for and administer individual requests for release or disclosure of personal and/or protected information
T0908	Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements
T0909	Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed
T0910	Act as, or work with, counsel relating to business partner contracts
T0911	Mitigate effects of a use or disclosure of personal information by employees or business partners
T0912	Develop and apply corrective action procedures
T0913	Administer action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel
T0914	Support the organization's privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations
T0915	Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations
T0916	Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units
T0917	Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices
T0918	Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations
T0919	Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials

Table 16: Task list of NICE Privacy Officer/Privacy Compliance Manager role (*Table source: https://www.nist.gov/file/372581)*

List of Abbreviations

Abbreviation	Translation
ADM	Systems Administration
AI	Artificial Intelligence
AN	Analyze
ANA	System Analyze
ARC	Systems Architecture
ASA	All-Source Analysis
BUT	Brno University of Technology
CAPE	SPARTA project Program #2: Continuous assessment in polymorphous environments
CDA	Cyber Defence Analysis
CEN	European Committee for Standardization
CEO	A chief executive officer
CIO	Chief Information Officer
CIR	Incident Response
CKMS	Crypto Key Management System
CLO	Collection Operations
CNSSI	Committee on National Security Systems
CO	Collect and Operate
COMSEC	Communications Security
CS	Cybersecurity
CSF	Cybersecurity framework
CUI	Controlled Unclassified Information
CWDI	Cybersecurity Workforce Development Initiative
DDoS	Distributed denial-of-service
DEV	Software Development
DLT	Distributed Ledger Technology

Abbreviation	Translation
DoDAF	Department of Defense Architecture Framework
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DRM	Digital Rights Management
DTA	Data Administration
EC	European Commission
e-CF	European e-Competence Framework
ECSO	European Cyber Security Organization
EGC	European Government CERTs group
ENISA	European Union Agency for Cybersecurity
EQF	European Qualifications Framework
EU	European Union
EXL	Executive Cyber Leadership
EXP	Exploitation Analysis
FEAF	Federal Enterprise Architecture Framework
FOR	Digital Forensics
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IAM	Identity and Access Management
ICS	Industrial control systems
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IMT	Institut Mines-Telecom
IN	Investigate
INF	Cyber Defense Infrastructure Support
INV	Cyber Investigation
IR	Incident Response

Abbreviation	Translation
ISC	(ISC)², Inc
IT	Information technology
JCCI	Joint Centre of Competence Infrastructure
JRC	Joint Research Centre
Kas	Knowledge Areas
KMG	Knowledge Management
KSAs	Knowledge, Skills, and Abilities
KTU	Kaunas University of Technology
L3CE	Lithuanian Cybercrime Center of Excellence for Training, Research & Education
LGA	Legal Advice and Advocacy
LNG	Language Analysis
MGT	Cybersecurity Management
MSs	Member States
NET	Network Services
NGO	Non-profit organization
NICE	National Initiative for Cybersecurity Education
NIS Directive	Directive on security of network and information systems
NIST	National Institute of Standards and Technology
OM	Operate and Maintain
OPL	Cyber Operational Planning
OPS	Cyber Operations
OV	Oversee and Govern
PHI	Personal Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PMA	Program/Project Management
PR	Protect and Defend

Abbreviation	Translation
RFID	Radio-frequency identification
RSK	Risk Management
SCADA	Supervisory control and data acquisition
SYS	Systems Development
SMEs	Small and medium-sized enterprises
SPP	Strategic Planning and Policy
SRP	Systems Requirements Planning
STS	Customer Service and Technical Support
TEA	Training, Education, and Awareness
TGT	Targets
TOGAF	Open group architecture framework
TRD	Technology R&D
TST	Test and Evaluation
TWA	Threat Analysis
UKON	Universitat Konstanz
UTARTU	Tartu Ulikool
VAM	Vulnerability Assessment and Management
WP	Work package