Horizon 2020 Program (2014-2020)
Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

CONCORDIA[1] Workshop on Education for cybersecurity professionals - post workshop report -

Abstract:

The purpose of this document is to present the results of the CONCORDIA Workshop on Education for Cybersecurity Professionals[2] organized online on June 2nd-3rd, 2020.

The workshop ran in the framework of the CONCORDIA project, linked to the activities on developing (1) a framework for skills certification and (2) course content creation for cybersecurity professionals[3]. All the presentations used during the event are available online on the CONCORDIA website and could be accessed individually via the specific session titles from the workshop Agenda.

Editor	*Felicia Cutas*
Contributors	*EIT Digital – Felicia Cutas, Muluneh Oli* *UT – Robert Muster* *TUVA - Argyro Chatzopoulou* *UNIMI – Marco Anisetti* *UL – Thibault Cholez, Remi Badonnel* *UZH - Muriel Franco, Bruno Rodriguez*

1 This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927

2 https://www.concordia-h2020.eu/workshops/workshop-education-2020/

3 The CONCORDIA workshop on Education for Cybersecurity Professionals brought together 7 CONCORDIA partners, and was led by EIT Digital. It was organized as part of the Task T3.4 (Establishing an European Education Ecosystem for Cybersecurity) and built on the effort and/or outcomes of the tasks T5.3 (Certification and Standardization activities – led by TUVA with contribution from UP), T4.1 (Working groups in technology domains of interest – led by UMIL with contribution from UL) and T4.3 (Economic perspectives – led by UZH). The platform used to collect data was built by UT.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

OBJECTIVES OF THE WORKSHOP 5

PARTICIPANTS TO THE WORKSHOP 5

STRUCTURE OF THE WORKSHOP 7

RESULTS OF THE WORKSHOP 8

DAY 1 - CYBERSECURITY CONSULTANT PROFILE – WHAT KNOWLEDGE AND SKILLS? - HANDS-ON EXERCISE 8
DAY 2 - PILOTING THE COURSE FOR THE CYBERSECURITY CONSULTANT PROFILE 11
LEARNING OBJECTIVE 1 – THREATS – WHAT KNOWLEDGE AND SKILLS? HANDS-ON EXERCISE 11
LEARNING OBJECTIVE 2 – TECHNOLOGY – WHAT KNOWLEDGE AND SKILLS? HANDS-ON EXERCISE 13
LEARNING OBJECTIVE 3 – ECONOMICS AND BUSINESS – WHAT KNOWLEDGE AND SKILLS? HANDS-ON EXERCISE 17
KNOWLEDGE AND SKILLS SPECIFIC AND IMPORTANT PER LEARNING OBJECTIVES – TELECOM INDUSTRY 19

NEXT STEPS 21

ANNEX 1: COMMUNICATION ACTIVITIES 22

ANNEX 2: AGENDA OF THE 2 HALF-DAYS' WORKSHOP 27

ANNEX 3: THE ROLE PROFILE OF THE CYBERSECURITY CONSULTANT 29

THE CYBERSECURITY CONSULTANT PROFILE – NICE FRAMEWORK 29
THE CYBERSECURITY CONSULTANT PROFILE – E-CF 30

ANNEX 4: THREATS AND SKILLS PER LEARNING OBJECTIVE – TOTAL VOTES 32

ANNEX 5: SCORING OF TOP 10 KNOWLEDGE AND SKILLS PER LEARNING OBJECTIVE – TELECOM INDUSTRY 37

Executive Summary

The work described within this document is mainly built around the outcomes of the different hands-on exercises. It reflects the efforts invested by the project team in (1) the determination of the Role Profile of the Cybersecurity Consultant and in (2) the definition of the content for previously defined Learning Objectives for the implementation of the relevant course, tailored per industries.

The project team faced the following challenges before the implementation of this workshop:

1) The Role of the Cybersecurity Consultant has been internationally identified but there is a lack of a concrete definition of the profile in all identified frameworks. To overcome this problem the project team had (though various processes) derived a proposal, which needed to be validated by the market.
2) In order to construct an effective and relevant to the market training course, it is of paramount importance to determine the Learning Objectives, the content to be covered considering the chosen Role Profile, and their variation between the different industries (the CONCORDIA project focuses on: Telecom, Finance, eHealth, Defense, Transport). The project team had already determined a definition of the Learning Objectives (Threats, Technology, Economics & Business) but needed the different opinions of industry representatives with respect to the main content to be offered for the specific Role of the Cybersecurity Consultant in terms of knowledge and skills, ranked for each industry.

The implementation of the workshop, produced the following results respectively:

1) The proposed 200 Knowledge and 90 Skills were validated and filtered down. The results of the workshop provided a ranking of the Knowledge and skills. By filtering the ranking results and further processing, the new Role Profile of the Cybersecurity Consultant was derived. The Role Profile is expressed in two different formats (based on the EU e-CF and based on the US NICE framework). The Role profile (EU e-CF) contains 13 Tasks and 15 e-competencies. The competences cover all five e-CF areas although there only one identified e-competence from the Run area, while all others are mostly balanced between the rest of the areas. This validates also the Mission of the Cybersecurity Consultant - providing advisory and technical expertise to help the client organizations design, implement, operate, control, maintain and improve their cybersecurity controls and operations.
2) The top 20 knowledge and top 10 skills per Learning Objective were further filtered down with respect to their relevance to specific CONCORDIA related industries. Looking into the results collected per Learning Objective, and with a specific focus on Telecom industry (the subject of the first pilot course) we have come to the following conclusions:
   a) Learning Objective 1 – Threats: the outcome of the workshop underline i) the need of basics knowledges on threats, vulnerabilities and CIA triad in connection to risk assessment and ii) the skills to apply such basic knowledges for an effective creation of security policies and risk evaluation to anticipate threats and mitigate risks. The workshop also underlined the importance of communicating the threats to the management board and identify and apply countermeasures based on basics knowledges on how a cyber-attack take place.

b) Learning Objective 2 – Technology: the workshop points out the importance of mastering the networking environment and the components to be protected, as well as acquiring knowledge and skills related to security management in terms of both assessment and configuration. The overall technology ranking highlights big data, internet-of-things, and artificial intelligence as major topics of interest, followed by mobile devices and cloud computing. This is in phase with the current evolution of the Internet which can be seen as a great integration platform for interconnecting multiple and heteregoneous entities, from connected devices to data center resources, and building complex and value-added secure systems.
c) Learning Objective 3 - Economics and Business: the analysis of the knowledge and skills selected indicates a high importance of abilities to understand not only cybersecurity main concepts and trends (for both vulnerabilities and protections) but also regulations and laws that impacts on the business and its operation. Thus, an in-depth understanding of the organization environment, processes, and exposed threats is critical to provide an effective analysis related to the economic impacts of cybersecurity on that.

The project team will use the resulting Role of the Cybersecurity Consultant to develop courses targeting this profile - tailored for the needs of specific industries, and to pilot the CONCORDIA Cybersecurity skills certification framework. The pilot on certification is expected to be tried out after the implementation of the relevant CONCORDIA pilot training course, in Q4 2020.

Objectives of the workshop

The CONCORDIA workshop objective was twofold:

1. To share with the participants our work so far in terms of Feasibility study on Skills Certification Schemes[4] and on the Methodology for developing courses for cybersecurity professionals[5]
2. To collect feedback regarding the matrix of knowledge and skills describing the European Cybersecurity Consultant profile and on the specific needs in terms of education for this specific profile, as a basis for developing future courses.

In preparation of this workshop we run two surveys:

1. Survey on Certification and Courses[6] run between February 18th – February 29th which helped collect initial input on the importance of certification of Cybersecurity skills, the relevance of the Cybersecurity Consultant profile for different industries/sectors, and on the learning objectives relevant for the development of new courses for this profile.
2. Participate in the definition of the European Cybersecurity Consultant profile[7] run between May 11th – May 31st which helped collect structured input on the degree of importance of different knowledge and skills associated to the Cybersecurity Consultant profile. As a support tool to collect the input we have developed a CONCORDIA specific platform[8] which was further used to run the hands-on exercises during the workshop.

Participants to the workshop

We looked into engaging mainly with European cybersecurity professionals, middle managers and executives from all sizes of organizations, representatives of national and European public institutions having an interest in Education for cybersecurity, international organisations active in cybersecurity area and universities offering or intending to include in their offer short courses for professionals.

The Registration process opened two weeks prior to the workshop, and we managed to collect 88 registrations in total out of which almost 48% came from industry and industry associations, our main target audience.

4 https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-SkillsFeasibilityStudy-forpublication.pdf
5 Methodology for developing courses for cybersecurity professionals
6 https://ec.europa.eu/eusurvey/runner/ConcordiaCertificationCourses
7 https://www.concordia-h2020.eu/news/participate-in-the-definition-of-the-european-cybersecurity-consultant-profile/
8 https://concordia.monitorboard.nl/

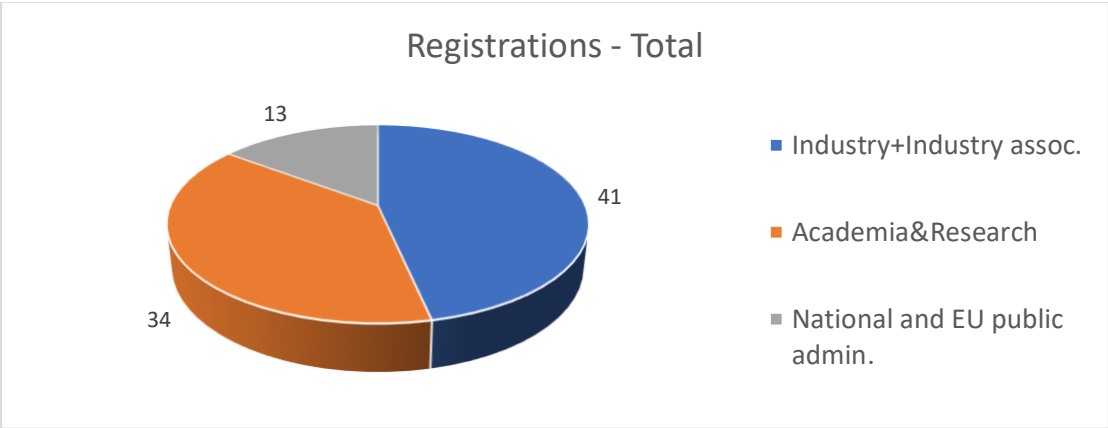


Figure 1. The distribution of Registrations per different groups of target audience

Out of this number of registered people only part of them joined the online sessions. Yet the percentage per categories stayed pretty much the same.

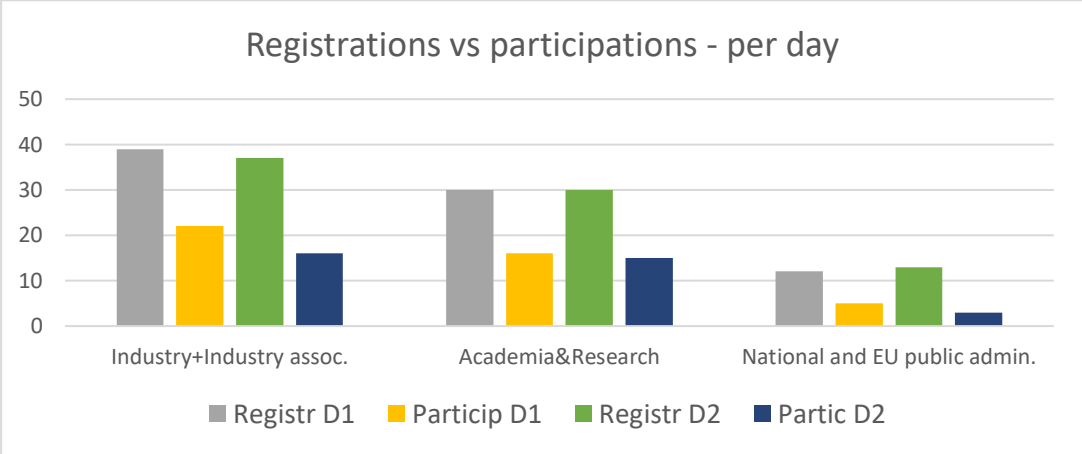


Figure 2. Registrations vs. Participations – per day, per group of target audience

In view of reaching this audience we used different communication channels, from the CONCORDIA website and its social media accounts to direct e-mail invitations distributed within the CONCORDIA partners professionals' networks. Special care was given to extend the invitations also to members of the other 3 cybersecurity pilots: SPARTA, ECHO and Cybersec4Europe.

CONCORDIA webpage of the event[9] registered until June 8th no less than 710 unique page views with the time spent by the visitors of about 4' minutes per session, a sign that the content displayed there was of interest.

EIT Digital as the coordinator of the event, leveraged its communication channels to spread the information in its ecosystem.

More statistics on the communication effort can be found in **Annex 1**.

Apart of the general online communication, we engaged with the registered people prior to the event by sending via email:

9 https://www.concordia-h2020.eu/workshops/workshop-education-2020/

- Few days in advance - the technical details for the virtual room connection and the link to the updated version of the agenda, and
- On the days of the workshop, half an hour before the start - additional information regarding the platform to be used during the hands-on exercise and about the different communication means.

Structure of the workshop

The workshop was organized in two parts and ran in two consecutive half-days:

Day 1 – looked into engaging with the audience for defining the European Cybersecurity Consultant profile in terms of knowledge and skills, and on collecting feedback on a new Cybersecurity Skills Certificate Framework

The specific objectives of the Day 1 were:

- Share with the participants the feasibility study outcome on cybersecurity certification
- Share with the participants the basic principles and components of the proposed CONCORDIA Cybersecurity Skills Certification Framework
- Share with the participants the approach of the EIT Label certification
- Share the survey results on the importance of Cybersecurity Skills Certification
- Present the process for the selection of the Cybersecurity Consultant Role as a pilot for the CONCORDIA Cybersecurity Skills Certification Framework and allow the participants to rank and validate the derived skill and knowledge sets

The Day 1 workshop was split into two parts:

- The first part described the roadmap followed by the project team from the initial concept of the need for Cybersecurity professionals to the CONCORDIA Cybersecurity Skills Certification Framework including the EIT Label certificate model.
- The second part provided the participants, the ability to view the skills and knowledge derived by the project team for the Role Profile of the Cybersecurity Consultant and to rank them based on their importance. Moreover, in this second part of the workshop, the steps regarding the rationale behind the selection of the Cybersecurity Consultant as well as the project team's view regarding the Roles function were provided to the participants.

Day 2 – took a step further and looked into developing Courses for Cybersecurity professionals and presented a new model for their deployment while also collecting feedback on the content for a pilot course addressing the Cybersecurity Consultant profile.

The specific objectives of Day 2 were:

- Share with the participants the CONCORDIA process for developing courses for professionals
- Share with the participants the results of the survey related to the knowledge and skills a Cybersecurity Consultant should have or develop in order to perform in a company

- Collect feedback on the knowledge and skills important to be covered in a course for the Cybersecurity Consultant profile, while also considering the different industries specificities.

The Day 2 was split in two parts:

- The first part described the Process for creating content for courses targeting cybersecurity professionals
- The second part was comprised of 3 sessions built around the 3 main learning objectives to be addressed in the future courses for Cybersecurity Consultant profile: Threats, Technology, Business & Economics. During these sessions the participants were invited to participate in hands-on exercises by ranking for each of the 3 learning objective the related knowledge and skills based on their relevance to the specific CONCORDIA industries: Telecom, Finance, eHealth, Transport, Defence.

The full agenda is presented in the **Annex 2**.

Results of the workshop

Day 1 - Cybersecurity Consultant profile – What Knowledge and Skills? - Hands-on exercise

The workshop had, on average, 50 participants, 28 of which took part in the ranking of the skills and knowledge (second part of the workshop). It should be noted that the platform was open to the public from the 13th of May 2020 to the day after the workshop, in order to collect the maximum amount of feedback. The figures shown below in this document and based on which the conclusions are derived, have used as input all users (before, during and after the workshop – 63 participations).

Through the hands-on exercise the existing 90 Skills and 200 Knowledge proposed by CONCORDIA project team were ranked based on their importance for the effective performance of the Role of the Cybersecurity Consultant.

The results of the ranking process are given as follows:

Knowledge

From the total number of votes (8780):

1854 were cast for Knowledge that was deemed Not important
4188 were cast for Knowledge that was deemed Important
2738 were cast for Knowledge that was deemed Very important

6 Knowledge were ranked as Not important by more than 50% of the voters
42 Knowledge were ranked as Important by more than 50% of the voters
34 Knowledge were ranked as Very important by more than 50% of the voters

Furthermore, during the hands on ranking of the knowledge of the Cybersecurity Consultant Role Profile, the following knowledge was proposed to be added with a degree of importance from 1 to 3, 3 being the highest:

Entity Name	Type	Importance
complexity and systems thinking	Knowledge	3

The project team analyzed the proposals and the relevant decision is given in the following table:

Entity Name	Decision
complexity and systems thinking	There is no clear Knowledge behind this entity - Discarded

The graphic presentation of the knowledge ranking is given below.

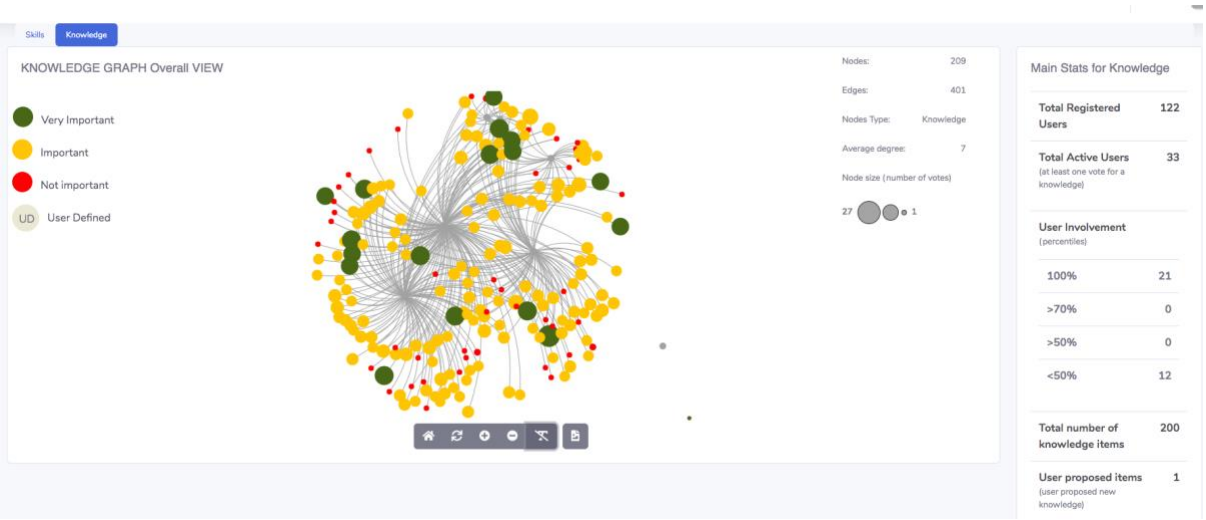


Figure 3. Network view of the Knowledge based on their importance

Skills

From the total number of votes (2960):

643 were cast for Skills that were deemed Not important
1305 were cast for Skills that were deemed Important
1012 were cast for Skills that were deemed Very important

5 Skills were ranked as Not important by more than 50% of the voters
29 Skills were ranked as Important by more than 50% of the voters
22 Skills were ranked as Very important by more than 50% of the voters

Additionaly, during the hands on ranking of the skills and knowledge of the Cybersecurity Consultant Role Profile, the following skills were proposed to be added with a degree of importance from 1 to 3, 3 being the highest:

Entity Name	**Type**	**Importance**
categoric learning	Skill	3
Chief Product Security Officer	Skill	3
cooperation	Skill	3
Skill applying a system view of the processes and objectives of the organization	Skill	3

Skill in mapping implemented security measures and controls	Skill	3
strategic thinking	Skill	3
systems and complexity thinking	Skill	3
Understanding organizational process	Skill	3

The project team analyzed the proposals and the following table shows the relevant decisions

Entity Name	Decision
categoric learning	Not clear - Discarded
Chief Product Security Officer	Not a Skill - Discarded
cooperation	The vote was allocated to the following: Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
Skill applying a system view of the processes and objectives of the organization	The vote was allocated to the following: Skill to use critical thinking to analyze organizational patterns and relationships.
Skill in mapping implemented security measures and controls	The vote was allocated to the following: Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
strategic thinking	The vote was allocated to the following: Skill to use critical thinking to analyze organizational patterns and relationships.
systems and complexity thinking	The vote was allocated to the following: Skill to use critical thinking to analyze organizational patterns and relationships.
Understanding organizational process	The vote was allocated to the following: Skill to use critical thinking to analyze organizational patterns and relationships.

The graphic presentation of the skills ranking is as follows:

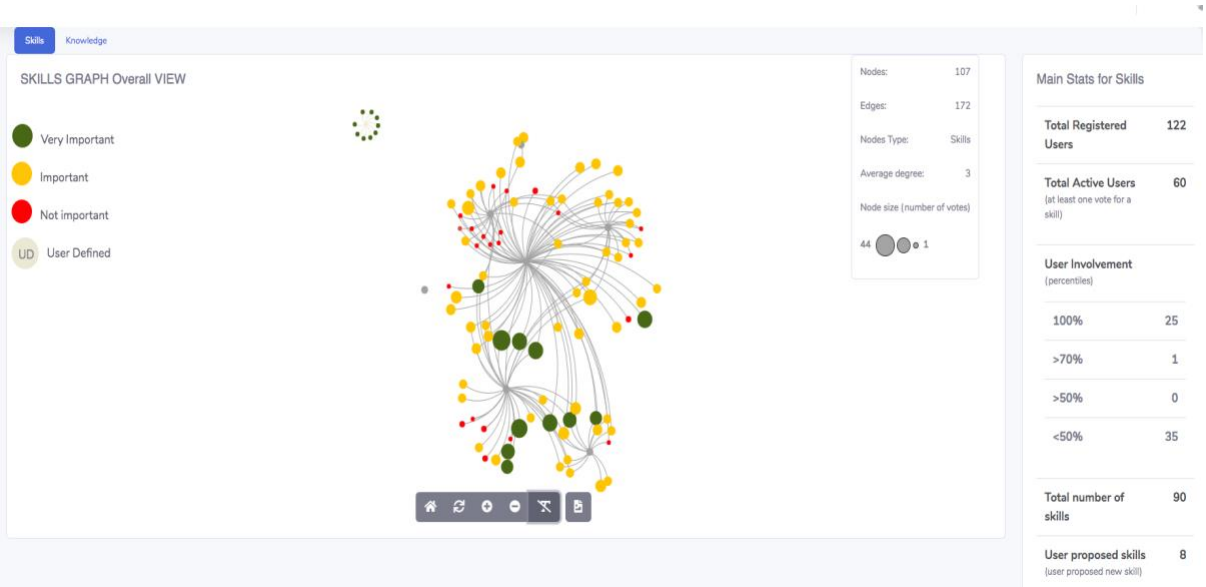


Figure 4. Network view of Skills based on their importance

The above-mentioned results regarding skills and knowledge were subsequently combined with the relevant abilities and tasks (for the NICE framework representation) and the relevant e-competencies (for the e-CF representation), and the two associated versions of the Role Profile of the Cybersecurity Consultant were derived. The final result is contained in Annex 3.

Day 2 - Piloting the course for the Cybersecurity Consultant profile

During these sessions we looked into further refine the input collected via the Survey in February (see description and reference in page 3) and during the Day 1 hands-on session mentioned above in order to come up with a list of knowledge and skills associated to individual learning objectives[10] and to specific industries[11].

In view of reaching this outcome we went through the following process:

- Prior to the workshop we analyzed the list of 90 skills and 200 knowledge characterizing the European Cybersecurity Consultant profile, and linked them to the relevant Learning Objectives (LO1 - Threats / LO2 - Technology / LO3 - Economics & Business).
- For each of the learning objectives we have displayed on the platform the top 10 skills and the top 20 knowledge selected by the users of the platform prior and during the workshop Day 1.
- For each of the learning objectives the participants were invited to vote on the relevance of the specific skills and knowledge for the individual industries listed[9].
- In case of the Learning Objective – Technology, and additional exercise was run in order to collect feedback on the most relevant technologies per industry.

The results presented below display the feedback gathered from the participants to the workshop related to the Telecom industry, the focus of the pilot to be deployed this year (2020). The full set of results covering all the industries considered for this exercise were included in **Annex 4**.

Learning Objective 1 – Threats – What Knowledge and Skills? Hands-on exercise

Learning Objective THREATS - Knowledge Row Labels	Sum of telecom
Knowledge of cyber threats and vulnerabilities.	8
Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	8
Knowledge of defense-in-depth principles and network security architecture.	8
Knowledge of an organization's threat environment.	7
Knowledge of confidentiality, integrity, and availability requirements.	7
Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	7
Knowledge of cybersecurity and privacy principles.	7
Knowledge of risk/threat assessment.	7
Knowledge of adversarial tactics, techniques, and procedures.	6
Knowledge of confidentiality, integrity, and availability principles.	6
Knowledge of cyber defense and information security policies, procedures, and regulations.	6
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	6

[10] The learning objectives were set as being linked to the "Threats", the "Technology" and the "Economics & Business" and were validated via the Survey.
[11] The industries selected for this exercise are the CONCORDIA industries: Telecom, e-Finance, e-Health, Transport/e-Mobility, Defence

Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	6
Knowledge of emerging security issues, risks, and vulnerabilities.	6
Knowledge of what constitutes a threat to a network.	6
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	5
Knowledge of security management.	5
Knowledge and understanding of operational design.	4
Knowledge of current and emerging threats/threat vectors.	4
Knowledge of information technology (IT) risk management policies, requirements, and procedures.	4
Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	4
Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	3
Knowledge that technology that can be exploited.	3

The ranking of top knowledges (8 or seven votes) related to threats for the Telecom industrial sector points out on one side basics fundamental knowledges related to cybersecurity and privacy principles and their connection with risk and threat assessment and on the other side very specific knowledges on defense-in-depth principles and network security architecture. It is in general evident the importance (from 6 to 5 votes) of fundamental knowledges like threats and vulnerabilities, CIA triad (Confidentiality, Integrity and Availability) and their tailoring to the organization environment as well as knowledge on how a cyber-attacks take place and how to set up an effective defence. As a general remark it is quite clear that the increment of software components and virtualization approaches in the telecom industries is reflected in this results as an increment of interest in basics knowledges on threats landscape, compared to very specific network related threats knowledges that are still mentioned as important but at the same level with basics and cross cutting knowledges.

Learning Objective THREATS - Skills Row Labels	Sum of telecom
Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	12
Skill in assessing security systems designs.	12
Skill in applying confidentiality, integrity, and availability principles.	11
Skill in designing countermeasures to identified security risks.	11
Skill to anticipate new security threats.	11
Skill in creating policies that reflect system security objectives.	10
Skill in performing impact/risk assessments.	10
Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	9
Skill in evaluating the adequacy of security designs.	9
Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	8

The ranking of top skills related to threats with respect to the Telecom industrial sector shows the importance (12 or 11 votes) of the assessment skills and risk identification and mitigation (e.g., countermeasures). It is evident also the importance of being capable to apply the CIA triad principles, the capability to create policies that reflects clear security objectives and of anticipating threats. We also note that soft skills for communicating threats with the management and board members is considered important (9 votes) as well; these points back to the importance of risk analysis supported by assessment to provide evidences for the decision makers at the company board level.

Learning Objective 2 – Technology – What Knowledge and Skills? Hands-on exercise

Learning Objective TECHNOLOGY - Skills Row Labels	Sum of telecom
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	9
Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	8
Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	7
Knowledge of defense-in-depth principles and network security architecture.	7
Knowledge and understanding of operational design.	6
Knowledge of authentication, authorization, and access control methods.	6
Knowledge of countermeasure design for identified security risks.	6
Knowledge of current and emerging cyber technologies.	6
Knowledge of cyber threats and vulnerabilities.	6
Knowledge of cybersecurity and privacy principles and methods that apply to software development.	6
Knowledge of cybersecurity and privacy principles.	6
Knowledge of information technology (IT) architectural concepts and frameworks.	6
Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	6
Knowledge of security management.	6
Knowledge of confidentiality, integrity, and availability requirements.	5
Knowledge of information technology (IT) risk management policies, requirements, and procedures.	5
Knowledge that technology that can be exploited.	5
Knowledge of confidentiality, integrity, and availability principles.	4
Knowledge of information security systems engineering principles (NIST SP 800-160).	4
Knowledge of computer networking concepts and protocols, and network security methodologies.	2
Knowledge of industry technologies' potential cybersecurity vulnerabilities.	2
Knowledge of cyber defense and vulnerability assessment tools and their capabilities.	1
Knowledge of industry standard security models.	1
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	1

The selected knowledge are very heterogeneous. For a better reading we can list them according to the six different topics they cover:

1. CYBERSECURITY:
    - Knowledge of cybersecurity and privacy principles.

- Knowledge of current and emerging cyber technologies (SIEM Security Information and Event Management, machine learning).
- Knowledge of countermeasure design for identified security risks.
- Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
- Knowledge of cybersecurity and privacy principles and methods that apply to software development. (safe memory management, how to deal with user input, etc.)

2. SECURITY MANAGEMENT:
   - Knowledge of security management
   - Knowledge of information technology (IT) risk management policies, requirements, and procedures.
   - Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
3. NETWORK SECURITY
   - Knowledge of defense-in-depth principles and network security architecture.
   - Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
4. THREATS INTELLIGENCE
   - Knowledge of cyber threats and vulnerabilities.
   - Knowledge that technology that can be exploited.
5. SECURITY PROPERTIES & AUTHENTICATION:
   - Knowledge of confidentiality, integrity, and availability principle.
   - Knowledge of confidentiality, integrity, and availability requirements. (encryption, replication)
   - Knowledge of access authentication methods.(Single-factor vs multi-factor, 802.1X, RADIUS, biometrics)
   - Knowledge of authentication, authorization, and access control methods.
6. INFORMATION SYSTEM DESIGN & ENGINEERING:
   - Knowledge and understanding of operational design.
   - Knowledge of information technology (IT) architectural concepts and frameworks (Three-tier architecture).
   - Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.
   - Knowledge of information security systems engineering principles (NIST SP 800-160).

The ranking of top knowledge related to technology for the Telecom industrial sector points out knowledge on network security architecture concepts, including topology, protocols, components (9 votes), knowledge on system software and organizational design (8 votes), knowledge in determining how a security system should work and is affected by changes (7 votes), and knowledge on defense-in-depth principles and network security architecture (7 votes). These requirements suppose to master the networking environment and the components to be protected, including knowledge on IT architectural concepts and frameworks (6 votes) and knowledge and understanding on operational design (6 votes), but also to acquire knowledge (6 votes) and key concepts (5 votes) on security management.

If we compute the average relevance of each category, the resulting scores are as follow:

1. Cybersecurity = 6.2;
2. Security Management = 5.7;
3. Network Security = 8;
4. Threats Intelligence = 5.5;
5. Security Properties and authentication = 5;
6. Information System Design & Engineering = 4.75.

This may help to better focus the courses on the most relevant aspects regarding technologies like network security and cybersecurity.

Learning Objective TECHNOLOGY - Skills Row Labels	Sum of telecom
Skill in applying confidentiality, integrity, and availability principles.	7
Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	6
Skill in assessing security systems designs.	5
Skill in creating policies that reflect system security objectives.	5
Skill in designing countermeasures to identified security risks.	5
Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	5
Skill in evaluating the adequacy of security designs.	5
Skill in performing impact/risk assessments.	5
Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	4
Skill in designing security controls based on cybersecurity principles and tenets.	2
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	2
Skill in designing multi-level security/cross domain solutions.	1

The ranking of top skills related to technology with respect to the Telecom industrial sector shows the importance of applying the principles of confidentiality, integrity, and availability (7 votes), and of assessing security controls based on cybersecurity principles and tenets (6 votes). When analyzing further the considered skills, we retrieve a strong security management requirement in terms of both assessment and configuration, with skills on the determination of how the security system is working/should work (5 votes), the assessment of security impacts and risks (5 votes), but also the creation of policies that reflect system security objectives (5 votes), the adequacy of security systems designs (5 votes), and the design of countermeasures to identified security risks.

An additional exercise was run for the Learning Objective Technology in order to identify the most important technologies challenging specific industries. This outcome will be used when selecting the case studies to be used during the course.

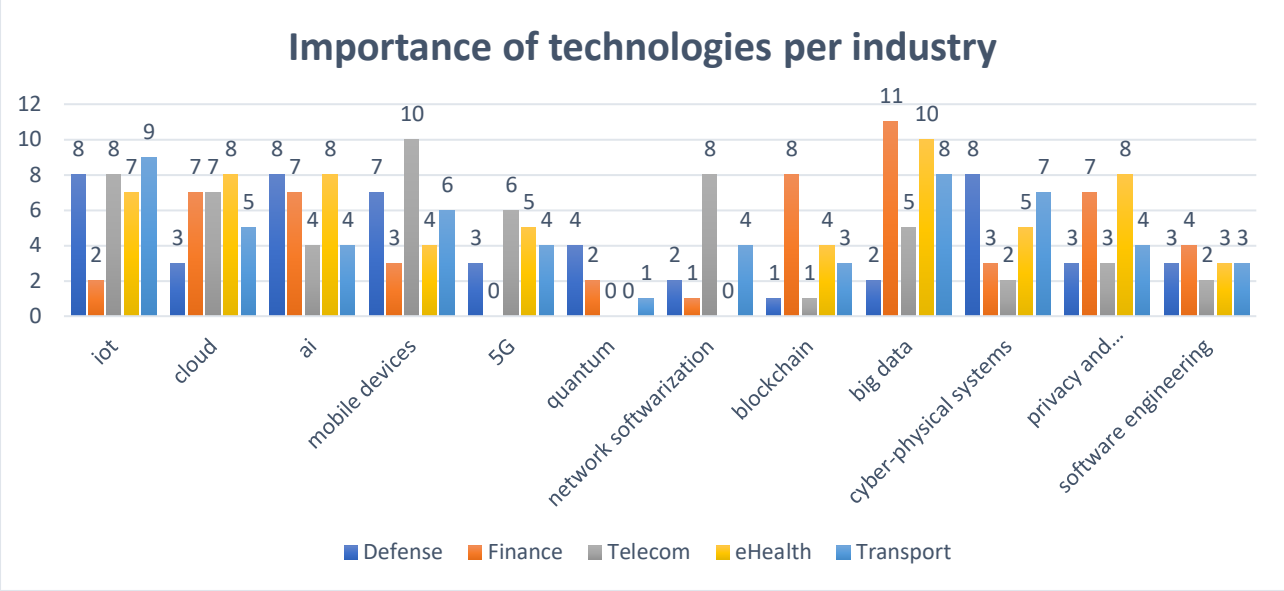


Figure 5. Importance of different technologies per industry – clustered per technologies

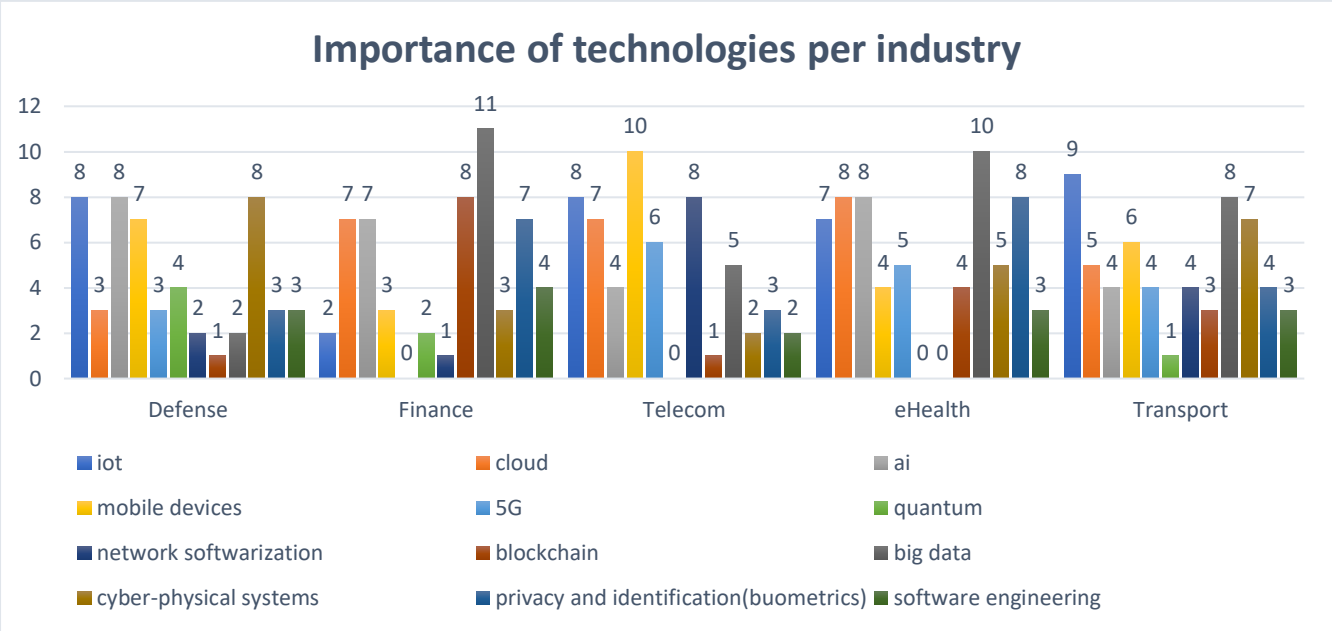


Figure 6. Importance of different technologies per industry – clustered per industries

The overall technology ranking highlights big data (36 votes in total), internet-of-things (34 votes in total), and artificial intelligence (31 votes in total) as major topics of interest, followed by mobile devices (30 votes in total) and cloud computing (30 votes in total). For the telecom industrial sector, the top-ranked technologies correspond respectively to mobile devices (10 votes), network softwarization (8 votes), and internet-of-things (8 votes), followed by cloud computing (7 votes). This is in phase with the current evolution of the Internet which can be seen as a great integration platform for interconnecting multiple and heteregoneous entities, from connected devices to data center resources, and building complex and value-added networked systems that require to be protected.

Learning Objective 3 – Economics and Business – What Knowledge and Skills? Hands-on exercise

Learning Objective ECONOMICS & BUSINESS - Knowkedge Row Labels	Sum of telecom
Knowledge of an organization's threat environment.	7
Knowledge of applicable business processes and operations of customer organizations.	7
Knowledge of confidentiality, integrity, and availability requirements.	7
Knowledge of cyber defense and information security policies, procedures, and regulations.	7
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	7
Knowledge of emerging security issues, risks, and vulnerabilities.	7
Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	7
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	7
Knowledge of confidentiality, integrity, and availability principles.	6
Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	6
Knowledge of cyber threats and vulnerabilities.	6
Knowledge of cybersecurity and privacy principles.	6
Knowledge of information security program management and project management principles and techniques.	6
Knowledge of security management.	6
Knowledge of what constitutes a threat to a network.	6
Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	5
Knowledge of organizational security policies.	5
Knowledge of organization's risk tolerance and/or risk management approach.	5
Knowledge of risk/threat assessment.	5
Knowledge and understanding of operational design.	2
Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	1
Knowledge of information technology (IT) risk management policies, requirements, and procedures.	1
Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.	1
Knowledge of Risk Management Framework (RMF) requirements.	1

The planning task is one of the most fundamental when it comes to cybersecurity, considering that anticipating situational awareness of possible incidents is the most efficient way to avoid them. Henceforth, the first step towards any planning involves the education of cybersecurity professionals, whose most relevant knowledge is listed in the Table above. According to the survey presented to professionals in the area, eight knowledge types were recognized as being most relevant, which are: knowledge of specific threats and vulnerabilities to the company's environment (7 votes), this logically involves knowledge of the business logic and operations of customers (7 votes). These two categories refer to the specific knowledge of the threats and vulnerabilities of the company and its customers, requiring experience from the professional

regarding the specific application. Other knowledge below refers to the basic concepts about cyber defense strategies, management of security policies, and compliance regulations (7 votes). Also, knowledge about privacy was listed in sequence (7 votes). Then, knowledge related to emerging threats was determined to be relevant (7 votes), denoting the need for cybersecurity professionals to be always up to date with the novel threats to which his system may, eventually, be exposed. In the last part of the most voted knowledge (with seven votes each), there is knowledge about the legislation to which the system is in force and organizational aspects. These determine, in general, obligations and determinations of the parties whose fundamental importance for a cybersecurity manager is reflected in the Table above.

Although with a minor overlap between categories of knowledge types listed in the Table, it is worth to note that less-specific knowledge on security in a broad sense (e.g., "knowledge of security management") were classified as relevant (6 votes), but not as much as relevant as previous ones, whose descriptions reflect specifics of business security (7 votes). Therefore, another seven knowledge was evaluated, with six votes dividing the second category of relevance to training cybersecurity professionals. Among these, we highlight general knowledge (i.e., not specific to the company's environment) about threats and vulnerabilities, knowledge of privacy principles, and what constitutes a threat to the network, are among those highlighted in this category. It is observed in this category of knowledge listed with six votes that despite referring to technical knowledge, they describe the general categories of knowledge about confidentiality, integrity, and availability. Thus, they are basic knowledge that these professionals must have to be able to apply it to a specific context of a company.

Similarly, the category of knowledge with five votes determines the third most relevant group of knowledge. These refer in general to organizational, legislative, and security policy knowledge except for knowledge about risk/threat assessment (5 votes). In these, similarly to the previous ones, a professional must be aware of the regulatory environment to which a system is inserted, as well as knowledge of risk assessment frameworks, tools for determining and managing policies, among others.

Among the knowledge listed in the Table above, those evaluated as of less relevance are: knowledge about the operational design of the business (2 votes), knowledge of how a security system should work (1 vote), general knowledge of security policy management risks in IT systems, knowledge of laws, authorities, restrictions, and regulations (1 vote), and requirements for applying risk management frameworks (1 vote). However, it is noted that despite being the least voted, this knowledge is still possible to be considered since they are part of top 10 relevant knowledge. It is also noted that more specific knowledge was, in general, better evaluated among the knowledge listed, showing that it is essential to build a solid theoretical base to know how to recognize threats and vulnerabilities but to know how they arise in specific scenarios within the operation logic of a company or customer.

Learning Objective ECONOMICS & BUSINESS - Skills Row Labels	Sum of telecom
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	8

Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	6
Skill to anticipate new security threats.	6
Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	5
Skill in creating policies that reflect system security objectives.	5
Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	5
Skill in performing impact/risk assessments.	5
Skill in writing about facts and ideas in a clear, convincing, and organized manner.	5
Skill to use critical thinking to analyze organizational patterns and relationships.	4
Skill in translating operational requirements into protection needs (i.e., security controls).	3
Skill in talking to others to convey information effectively.	2

The ranking of top skills related to economics & business concerning the telecom industrial sector shows the importance of understanding the protection needs of companies (8 votes) and planning activities related to the cybersecurity (6 votes). Also, skills associated with anticipating new security threats (6 votes) are relevant and directly related to effective planning. Next, skills related to communicating with all levels of management, creating security policies, performing risk assessments, and writing about ideas transparently and effectively shows relevant as well (5 votes each of them). Finally, the top skills consist of critical thinking to analyze organizational patterns and its relationships (4 votes), translating operational requirements into protection needs (3 votes), and talk to others to convey information (2 votes).

Therefore, by analyzing the knowledge and skills of learning objective Economics & Business, it indicates a high importance of abilities to understand not only cybersecurity main concepts and trends (for both vulnerabilities and protections) but also regulations and laws that impacts on the business and its operation. Thus, an in-depth understanding of the organization environment, processes, and exposed threats is critical to provide an effective analysis related to the economic impacts of cybersecurity on that.

Knowledge and Skills specific and important per Learning Objectives – Telecom Industry

Some Knowledge and Skills are very specific to one of the learning objectives identified (LO1 - Threats / LO2 - Technology / LO3 - Economics & Business) and they should be given priority when developing the course content. Other knowledge and skills are relevant to more than one learning objective and, if they are of high relevance for the targeted profile, they could be addressed in the course from different angles.

When looking into identifying the most relevant knowledge and skills per specific learning objective as compared to the others, based on the feedback received during the workshop, we observe the following with respect to the Telecom Industry:

Knowledge:

1. very important for LO1 (score 6 and 8) but not important for LO2 and LO3 (score 0)

- Knowledge of adversarial tactics, techniques, and procedures.
- Knowledge of authentication, authorization, and access control methods.
- Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
- Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
- Knowledge of emerging security issues, risks, and vulnerabilities.

2. very important for LO2 (score 6 and 8) but not important for LO1 and LO3 (score 0)
- Knowledge of countermeasure design for identified security risks.
- Knowledge of current and emerging cyber technologies.
- Knowledge of cybersecurity and privacy principles and methods that apply to software development.
- Knowledge of information technology (IT) architectural concepts and frameworks.
- Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
- Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.

3. very important for LO3 (score 5,6,7) but not important for LO1 and LO2 (score 0)
- Knowledge of applicable business processes and operations of customer organizations.
- Knowledge of applicable business processes and operations of customer organizations.
- Knowledge of information security program management and project management principles and techniques.
- Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Knowledge of organization's risk tolerance and/or risk management approach.
- Knowledge of organizational security policies.

4. very important for all three learning objectives (score 5,6,7)
- Knowledge of cyber threats and vulnerabilities.
- Knowledge of cybersecurity and privacy principles.
- Knowledge of security management.

Skills:

1. very important for LO1 and LO2 (score 5-12) but not important for LO3 (score 0)
- Skill in applying confidentiality, integrity, and availability principles.
- Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
- Skill in assessing security systems designs.
- Skill in designing countermeasures to identified security risks.
- Skill in evaluating the adequacy of security designs.

2. very important for LO3 (score 6, 8) but not important for LO1 and LO2 (score 0)
   - Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.
   - Skill in discerning the protection needs (i.e., security controls) of information systems and networks.

3. very important for all three learning objectives (score 5-10)
   - Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
   - Skill in creating policies that reflect system security objectives.
   - Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
   - Skill in performing impact/risk assessments.

The full set of data for the Telecom industry is presented in **Annex 6**.

Next steps

Day 1:
The resulting Role Profile of the Cybersecurity consultant will be used as the basis of the 1st CONCORDIA Cybersecurity skills certification scheme. Within this year, the project team will design and start implementing the relevant certification scheme. A first pilot of the scheme is expected to be tried out after the implementation of the relevant CONCORDIA training course, in Q4.

Day 2:
The input collected during the workshop will be further used in developing courses targeting the Cybersecurity Consultant profile, based on the CONCORDIA methodology for developing courses for cybersecurity professionals. The first pilot is scheduled to be run by the end of year 2020 and will focus on Telecom industry. The course content will be then adapted to the Finance and e-Health industries and will run one in year 2021 and another one in year 2022.

Annex 1: Communication activities

A. Communication via the CONCORDIA channels:

The impact of the posts via the different social-media channels are as follows:

Twitter: 6 posts summing up 495 engagements and 13849 impressions

https://twitter.com/concordiah2020/status/1263425740781076480
https://twitter.com/concordiah2020/status/1263771426479374336
https://twitter.com/concordiah2020/status/1264843699554594816
https://twitter.com/concordiah2020/status/1265267189399027712
https://twitter.com/concordiah2020/status/1265611212802359297
https://twitter.com/concordiah2020/status/1265988576950566914

Facebook: 6 posts summing up 62 engagements and 1721 reaches

https://www.facebook.com/concordia.eu/photos/a.377656202820063/633807200538294/?type=3&theater
https://www.facebook.com/concordia.eu/photos/a.377656202820063/634351397150541/?type=3&theater
https://www.facebook.com/concordia.eu/photos/a.377656202820063/636065713645776/?type=3&theater
https://www.facebook.com/concordia.eu/photos/a.377656202820063/636731280245886/?type=3&theater
https://www.facebook.com/concordia.eu/photos/a.377656202820063/637260456859635/?type=3&theater
https://www.facebook.com/concordia.eu/photos/a.377656202820063/637886010130413/?type=3&theater

LinkedIn: 6 posts summing up 70 engagements and 2941 views

https://www.linkedin.com/posts/concordia-h2020_cybersecurity-europe-activity-6669191630848856064-oEfL
https://www.linkedin.com/posts/concordia-h2020_consultant-cybersecurity-certificate-activity-6669538055071793152-8dDO
https://www.linkedin.com/posts/concordia-h2020_cybersecurity-course-activity-6670609590511538176-Hwzn
https://www.linkedin.com/posts/concordia-h2020_european-cybersecurity-nist-activity-6671033915278413824-rIXZ
https://www.linkedin.com/posts/concordia-h2020_cybersecurity-activity-6671377053687787520-k4nC
https://www.linkedin.com/posts/concordia-h2020_cybersecurity-europe-activity-6671754512513961984-VxoL

The visuals used on Twitter, Facebook and LinkedIn were the same and they are displayed below.

concordia-h2020.eu
@concordiah2020

SAVE THE DATE! We organize an online Workshop on education for #cybersecurity professionals. It will take place on 2-3 June. A great opportunity for everyone who wants to participate in shaping this area of education in #Europe 😊 🇪🇺
Register here: concordia-h2020.eu/workshops/work...

DigitalSingleMarket and 9 others

2:05 PM · May 21, 2020 · Twitter Web App

34 Retweets **35** Likes

concordia-h2020.eu
@concordiah2020

You can still participate in defining #European #Cybersecurity Consultant profile! Click on the link and rank our compilation from the #NIST Workforce Framework. The results will be discussed at our online workshop which will take place on 2 June 😊
concordia.monitorboard.nl

DigitalSingleMarket and 5 others

4:03 PM · May 26, 2020 · Twitter Web App

5 Retweets **6** Likes

concordia-h2020.eu
@concordiah2020

The first part of our workshop will focus on defining the cybersecurity #consultant profile. We will also collect feedback on the #cybersecurity skills certificate framework. Register now and shape the future of #education for cybersecurity pros in Europe! concordia-h2020.eu/workshops/work...

EIT Digital and 9 others

12:59 PM · May 22, 2020 · Twitter Web App

10 Retweets **16** Likes

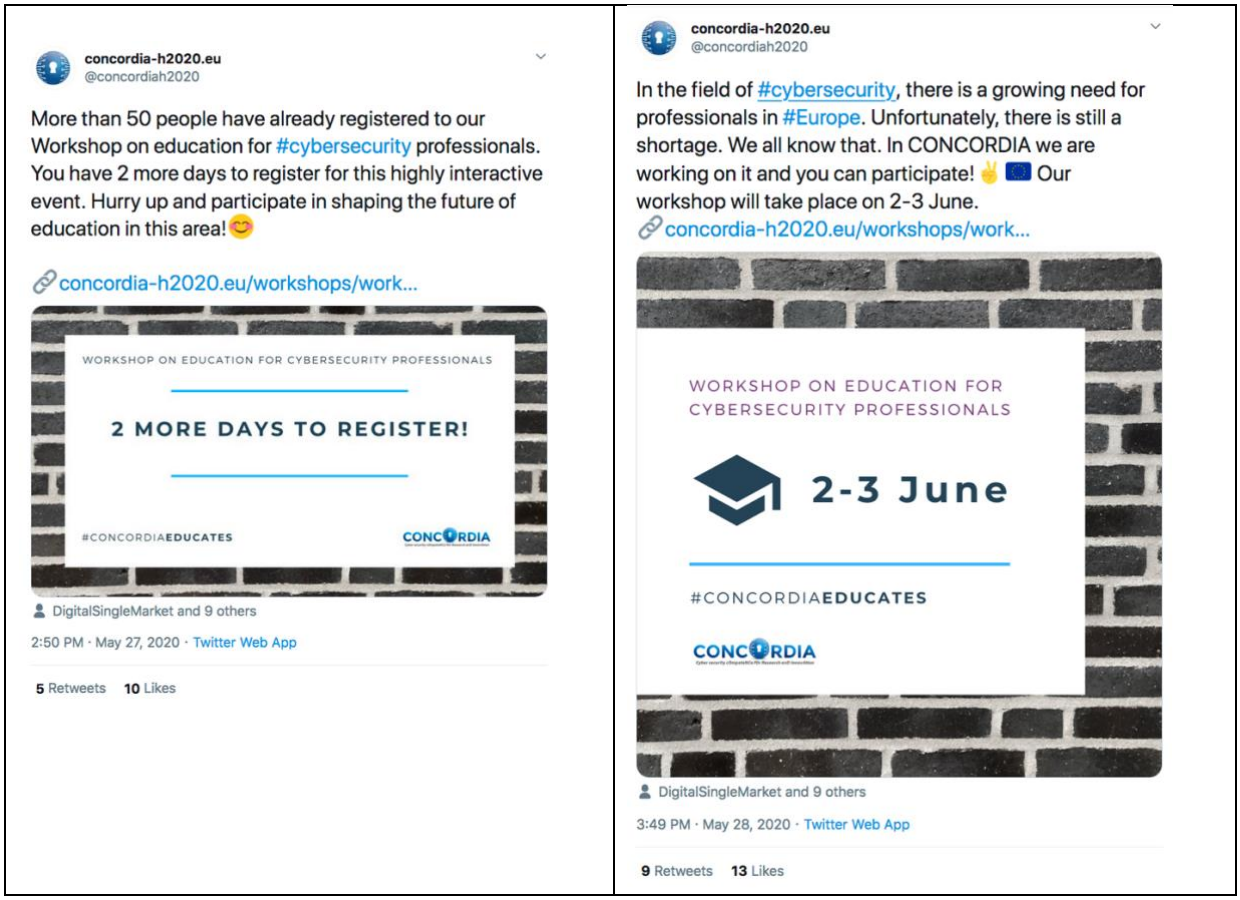
concordia-h2020.eu
@concordiah2020

The second part of our workshop takes a step further and looks into developing courses for #cybersecurity professionals and presenting a new model for their deployment while also collecting feedback on the content for a pilot #course 😊 Register here concordia-h2020.eu/workshops/work...

CyberSec_EU 🇪🇺 and 7 others

12:00 PM · May 25, 2020 · Twitter Web App

6 Retweets **17** Likes

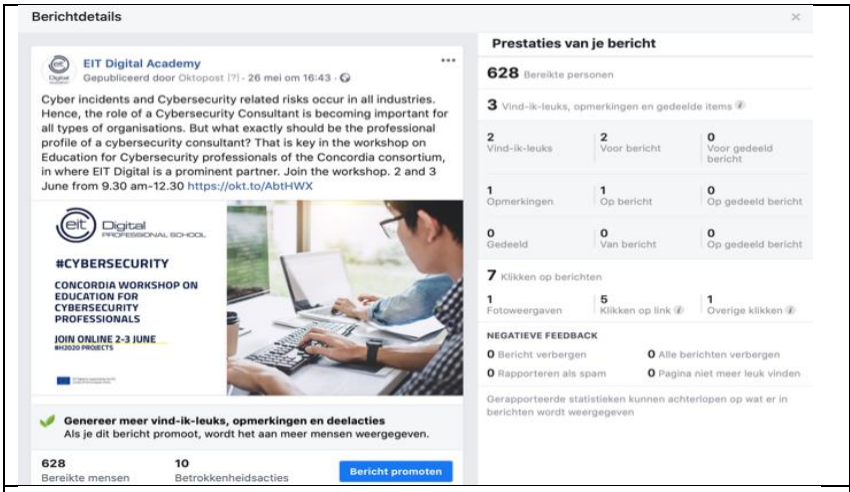
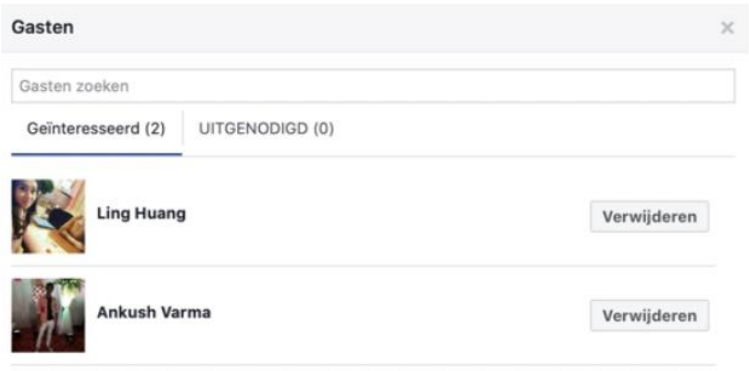


B. EIT Digital channels:

Website article: gained 32 views
https://www.eitdigital.eu/newsroom/events/article/concordia-workshop-on-education-for-cybersecurity-professionals/
https://professionalschool.eitdigital.eu/about-us/events/article/concordia-workshop-on-education-for-cybersecurity-professionals/

	Page	Page Views	Unique Page Views	Avg. Time on Page	Entrances
		32 % of Total: 0.02% (204,554)	27 % of Total: 0.02% (131,791)	00:02:11 Avg for View: 00:01:48 (21.66%)	9 % of Total: 0.01% (98,855)
1.	www.eitdigital.eu/newsroom/events/article/concordia-workshop-on-education-for-cybersecurity-professionals/	32 (100.00%)	27 (100.00%)	00:02:11	9 (100.00%)

Social Media

	Facebook message (EIT Digital Academy account): reached 628 persons, 7 people clicked on the message, 3 likes
	Facebook event item: two people said to be interested. Reach 179 people. 3 clicks to the event page
	Twitter EIT Digital account: 5 likes, 5 retweets
	Twitter EIT Digital Academy account (2793 followers): 2 likes 2 retweets

	LinkedIn (17,880) followers: 11 likes

Annex 2: *Agenda of the 2 half-days' workshop*

Part 1: June 2nd, 2020

Part 1: June 2nd, from 9:30 – 12:30 (CET Brussels time), online | **Part 2: June 3rd, from 9:30 – 12:30 (CET Brussels time), online**

Defining the Cybersecurity Consultant profile and collecting feedback on the Cybersecurity Skills Certificate Framework

Time (CET Brussels time)	Topic	Presenter
09:30 – 09:40 (10')	**Welcome and introductory remarks**	EIT Digital Felicia Cutas, Muluneh Oli
09:40 – 10:10 (30')	**CONCORDIA Feasibility study on Certifications schemes and the Skills Certification Framework**	TUV TRUST IT Argyro Chatzopoulou
10:10 – 10:40 (30')	**Piloting the certification framework – Defining the elements**	
10:10 – 10:20 (10')	• *Summary of the Certification related survey results*	EIT Digital Muluneh Oli
10:20 – 10:40 (20')	• *Introducing a Certification Framework for Professional Education*	EIT Digital Roberto Prieto
10:40 – 10:50 (10')	**Break**	
10:50 – 11:00 (10')	**Presentation of the CONCORDIA Cybersecurity skills application**	University of Twente Robert Muster
11:00 – 12:00 (60')	**Cybersecurity Consultant profile – What Knowledge and Skills?** Hands-on exercise	Moderator TUV TRUST IT Argyro Chatzopoulou University of Patras Kostas Lampropoulos
12:00 – 12:10 (10')	**Conclusions and next steps**	EIT Digital Muluneh Oli

Part 2 – June 3rd, 2020

Part 1: June 2nd, from 9:30 – 12:30 (CET Brussels time), online | **Part 2: June 3rd, from 9:30 – 12:30 (CET Brussels time), online**

Developing Courses for Cybersecurity professionals and collecting feedback on the pilot course for Cybersecurity Consultant profile

Time (CET Brussels time)	Topic	Presenter
09:30 – 09.35 (5')	**Welcome and introductory remarks**	EIT Digital Felicia Cutas
09:35 – 09:45 (10')	**Building an European Education Ecosystem for Cybersecurity in Europe – a cross pilots effort**	European Commission Rafael Tesoro-Carretero
09:45 – 10:00 (15')	**CONCORDIA process for creating a course for cybersecurity professionals**	EIT Digital Fabio Pianesi
10:00 – 12:10 (2h10')	**Piloting the course for the Cybersecurity Consultant profile**	Moderator EIT Digital
10:00 – 10:10 (10')	• *Results of the Survey defining courses for the Cybersecurity consultant profile*	EIT Digital Felicia Cutas
10:10 – 10:50 (40')	• *Learning Objective 1 – Threats – What Knowledge and Skills?* Hands-on exercise	University of Milan Marco Anisetti
10:50 – 11:00 (10')	**Break**	
11:00 – 11:40 (40')	• *Learning Objective 2 – Technology – What Knowledge and Skills?* Hands-on exercise	University of Lorraine Thibault Cholez, Rémi Badonnel
11:40– 12:20 (40')	• *Learning Objective 3 – Economics and Business – What Knowledge and Skills?* Hands-on exercise	University of Zurich Muriel Franco, Bruno Rodrigues
12:20 – 12:30 (10')	**Conclusions and next steps**	EIT Digital Felicia Cutas

Annex 3: The Role Profile of the Cybersecurity Consultant

The Cybersecurity Consultant Profile – NICE Framework

Work Role Name	Cybersecurity Consultant
Work Role ID	XXXXXXXXXX
Speciality Area	All-Source Analysis (ASA), Collection Operations (CLO), Customer Service and Technical Support (STS), Cyber Defense Analysis (CDA), Cyber Defense Infrastructure Support (INF), Cyber Investigation (INV), Cyber Operational Planning (OPL), Cyber Operations (OPS), Cybersecurity Management (MGT), Data Administration (DTA), Digital Forensics (FOR), Executive Cyber Leadership (EXL), Exploitation Analysis (EXP), Incident Response (CIR), Knowledge Management (KMG), Language Analysis (LNG), Legal Advice and Advocacy (LGA), Network Services (NET), Project Management/Acquisition and Program (PMA), Risk Management (RSK), Software Development (DEV), Strategic Planning and Policy (SPP), Strategic Planning and Policy Development (SPP), Systems Administration (ADM), Systems Analysis (ANA), Systems Architecture (ARC), Systems Development (SYS), Systems Requirements Planning (SRP), Targets (TGT), Technology R&D (TRD), Test and Evaluation (TST), Threat Analysis (TWA), Training, Education, and Awareness (TEA), Vulnerability Assessment and Management (VAM)
Category	Analyze (AN), Collect and Operate (CO), Investigate (IN), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Securely Provision (SP)
Work Role Description	Cybersecurity Consultants, provides advisory and technical expertise to help the client organizations design, implement, operate, control, maintain and improve their cybersecurity controls and operations.
Tasks	T0003, T0004, T0005, T0010, T0017, T0018, T0019, T0022, T0041, T0043, T0054, T0060, T0061, T0071, T0072, T0073, T0074, T0075, T0076, T0078, T0082, T0088, T0090, T0097, T0101, T0102, T0105, T0106, T0115, T0118, T0119, T0121, T0123, T0127, T0133, T0142, T0143, T0151, T0155, T0158, T0159, T0174, T0177, T0178, T0181, T0186, T0187, T0188, T0194, T0199, T0200, T0202, T0203, T0205, T0208, T0212, T0214, T0219, T0227, T0231, T0233, T0234, T0244, T0246, T0248, T0251, T0256, T0260, T0261, T0263, T0270, T0271, T0272, T0273, T0274, T0282, T0284, T0291, T0297, T0306, T0307, T0308, T0309, T0315, T0323, T0327, T0328, T0348, T0360, T0372, T0384, T0388, T0395, T0400, T0410, T0414, T0425, T0427, T0433, T0446, T0449, T0450, T0451, T0453, T0454, T0465, T0467, T0470, T0472, T0475, T0478, T0483, T0484, T0485, T0486, T0489, T0496, T0499, T0502, T0503, T0504, T0505, T0508, T0509, T0510, T0518, T0519, T0526, T0527, T0528, T0529, T0530, T0533, T0535, T0536, T0537, T0538, T0546, T0547, T0548, T0549, T0550, T0551, T0552, T0556, T0560, T0577, T0589, T0686, T0708, T0710, T0718,

	T0724, T0738, T0782, T0834, T0835, T0845, T0847, T0871, T0875, T0906, T0928
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0013, K0026, K0032, K0038, K0039, K0042, K0044, K0045, K0047, K0048, K0049, K0054, K0058, K0059, K0066, K0074, K0087, K0088, K0098, K0104, K0106, K0110, K0112, K0115, K0119, K0121, K0147, K0149, K0151, K0157, K0158, K0160, K0161, K0162, K0165, K0174, K0177, K0179, K0211, K0214, K0222, K0231, K0234, K0242, K0260, K0263, K0267, K0276, K0288, K0292, K0293, K0295, K0297, K0299, K0314, K0335, K0336, K0342, K0344, K0347, K0487, K0499, K0612, K0613
Skills	S0001, S0006, S0010, S0018, S0022, S0023, S0027, S0034, S0036, S0070, S0072, S0078, S0085, S0086, S0116, S0134, S0137, S0140, S0141, S0145, S0147, S0152, S0171, S0175, S0177, S0232, S0242, S0244, S0249, S0250, S0273, S0278, S0296, S0301, S0356, S0357, S0358, S0359
Abilities	A0001, A0004, A0006, A0009, A0011, A0013, A0014, A0015, A0018, A0033, A0047, A0048, A0052, A0055, A0057, A0058, A0062, A0064, A0070, A0074, A0082, A0083, A0085, A0088, A0092, A0093, A0094, A0095, A0096, A0106, A0108, A0110, A0118, A0119

The Cybersecurity Consultant Profile – e-CF

Profile Title	Cybersecurity Consultant		
Summary Statement	Provision of expert advice on Cybersecurity Issues		
Mission	Cybersecurity Consultants, provides advisory and technical expertise to help the client organizations design, implement, operate, control, maintain and improve their cybersecurity controls and operations.		
Deliverables	Accountable	Responsible	Contributor
	New cybersecurity measures integration proposal	Security requirements	Cybersecurity Related Policies, Procedures, Guidelines and Standards Risk Management Procedure and records Proposals regarding Cybersecurity controls Assessments and Audits Incident investigation Security Optimization
Main task/s	• Advise on Risk, Measures and Security Posture • Analyze and assess relevant practices and evaluate compliance • Advise on security optimization measures • Provide expert support on cybersecurity events and incidents • Design relevant cybersecurity policies, procedures, guidelines and standards • Test the organization's security posture • Develop cybersecurity designs • Evaluate and raise awareness of staff, provide education services.		

	• Analyze that assess relevant practices that evaluate compliance • Maintain current knowledge on relevant cybersecurity subjects and trends • Identify security requirements • Correct deficiencies • Conduct Risk Assessment		
e-Competences (from e-CF)	A5	Architecture Design	Level 5
	A6	Application Design	Level 1
	A7	Technology Trend Monitoring	Level 4
	B1	Application Development	Level 2
	B3	Testing	Level 3
	B6	ICT Systems Engineering	Level 4
	C4	Problem Management	Level 3
	D1	Information Security Strategy Development	Level 4
	D3	Education and Training Provision	Level 3
	D11	Needs Identification	Level 3
	E2	Project and Portfolio Management	Level 3
	E3	Risk Management	Level 4
	E4	Relationship Management	Level 3
	E8	Information Security Management	Level 3
	E9	Information Systems Governance	Level 4
KPI Area	Impact of advice in Cyber security implementation		

Annex 4: Threats and Skills per Learning Objective – total votes

Learning Objective THREATS - Knowledge Row Labels	Sum of telecom	Sum of eHealth	Sum of finance	Sum of defense	Sum of transport	Sum of general
Knowledge of cyber threats and vulnerabilities.	8	7	7	6	6	7
Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	8	9	9	5	6	5
Knowledge of defense-in-depth principles and network security architecture.	8	6	7	8	3	5
Knowledge of an organization's threat environment.	7	9	6	7	9	7
Knowledge of confidentiality, integrity, and availability requirements.	7	7	6	5	4	5
Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	7	6	7	7	5	7
Knowledge of cybersecurity and privacy principles.	7	7	6	3	3	4
Knowledge of risk/threat assessment.	7	6	7	6	4	6
Knowledge of adversarial tactics, techniques, and procedures.	6	2	7	7	3	3
Knowledge of confidentiality, integrity, and availability principles.	6	7	6	6	6	8
Knowledge of cyber defense and information security policies, procedures, and regulations.	6	7	7	7	5	6
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	6	7	6	3	5	2
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	6	1	4	4	2	4
Knowledge of emerging security issues, risks, and vulnerabilities.	6	4	6	5	4	6
Knowledge of what constitutes a threat to a network.	6	3	5	5	3	4
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	5	3	5	4	3	4
Knowledge of security management.	5	3	5	4	3	8
Knowledge and understanding of operational design.	4	4	3	2	4	4
Knowledge of current and emerging threats/threat vectors.	4	3	4	4	3	2
Knowledge of information technology (IT) risk management policies, requirements, and procedures.	4	4	3	4	2	5
Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	4	3	2	3	1	6
Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how	3	1	3	2	1	1

changes in conditions, operations, or the environment will affect these outcomes.						
Knowledge that technology that can be exploited.	3	2	3	3	2	1

Learning Objective THREATS - Skills Row Labels	Sum of telecom	Sum of eHealth	Sum of finance	Sum of defense	Sum of transport	Sum of general
Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	12	11	10	11	7	8
Skill in assessing security systems designs.	12	9	10	10	8	8
Skill in applying confidentiality, integrity, and availability principles.	11	12	11	9	6	10
Skill in designing countermeasures to identified security risks.	11	11	10	12	8	10
Skill to anticipate new security threats.	11	10	10	10	7	10
Skill in creating policies that reflect system security objectives.	10	12	10	7	7	10
Skill in performing impact/risk assessments.	10	14	10	9	8	8
Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	9	7	10	9	7	10
Skill in evaluating the adequacy of security designs.	9	10	9	10	7	9
Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	8	7	9	8	8	8

Learning Objective TECHNOLOGY - Knowkedge Row Labels	Sum of telecom	Sum of eHealth	Sum of finance	Sum of defense	Sum of transport	Sum of general
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	9	6	6	5	4	3
Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	8	6	7	5	4	2
Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	7	7	8	5	3	2
Knowledge of defense-in-depth principles and network security architecture.	7	4	6	5	5	2
Knowledge and understanding of operational design.	6	3	5	2	5	5
Knowledge of authentication, authorization, and access control methods.	6	6	6	3	6	5
Knowledge of countermeasure design for identified security risks.	6	3	5	3	2	4
Knowledge of current and emerging cyber technologies.	6	4	4	6	3	4
Knowledge of cyber threats and vulnerabilities.	6	4	5	5	2	4

Knowledge of cybersecurity and privacy principles and methods that apply to software development.	6	5	7	2	3	3
Knowledge of cybersecurity and privacy principles.	6	5	5	4	5	6
Knowledge of information technology (IT) architectural concepts and frameworks.	6	3	5	3	3	4
Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	6	5	5	4	3	3
Knowledge of security management.	6	5	6	3	3	4
Knowledge of confidentiality, integrity, and availability requirements.	5	6	5	4	3	4
Knowledge of information technology (IT) risk management policies, requirements, and procedures.	5	5	5	2	3	5
Knowledge that technology that can be exploited.	5	4	3	3	2	3
Knowledge of confidentiality, integrity, and availability principles.	4	6	7	2	3	3
Knowledge of information security systems engineering principles (NIST SP 800-160).	4	3	3	5	3	3
Knowledge of computer networking concepts and protocols, and network security methodologies.	2	0	0	0	0	0
Knowledge of industry technologies' potential cybersecurity vulnerabilities.	2	2	1	2	2	2
Knowledge of cyber defense and vulnerability assessment tools and their capabilities.	1	1	1	0	1	0
Knowledge of industry standard security models.	1	1	1	1	1	1
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	1	2	2	2	1	1

Learning Objective TECHNOLOGY - Skills Row Labels	**Sum of telecom**	**Sum of eHealth**	**Sum of finance**	**Sum of defense**	**Sum of transport**	**Sum of general**
Skill in applying confidentiality, integrity, and availability principles.	7	7	7	6	4	6
Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	6	7	7	5	3	4
Skill in assessing security systems designs.	5	3	4	6	4	3
Skill in creating policies that reflect system security objectives.	5	6	7	3	3	4
Skill in designing countermeasures to identified security risks.	5	4	4	5	2	4
Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	5	4	4	4	2	5
Skill in evaluating the adequacy of security designs.	5	4	5	3	2	4
Skill in performing impact/risk assessments.	5	6	4	6	3	4
Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	4	4	5	4	2	6

Skill in designing security controls based on cybersecurity principles and tenets.	2	1	1	1	0	0
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	2	2	1	2	2	4
Skill in designing multi-level security/cross domain solutions.	1	2	2	2	0	2

Learning Objective ECONOMICS & BUSINESS - Knowkedge Row Labels	Sum of telecom	Sum of eHealth	Sum of finance	Sum of defense	Sum of transport	Sum of general
Knowledge of an organization's threat environment.	7	6	7	4	5	3
Knowledge of applicable business processes and operations of customer organizations.	7	5	6	1	3	2
Knowledge of confidentiality, integrity, and availability requirements.	7	6	7	3	6	5
Knowledge of cyber defense and information security policies, procedures, and regulations.	7	7	7	5	3	5
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	7	6	7	1	3	2
Knowledge of emerging security issues, risks, and vulnerabilities.	7	5	6	3	4	3
Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	7	7	8	6	8	2
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	7	7	7	4	6	4
Knowledge of confidentiality, integrity, and availability principles.	6	7	6	3	3	6
Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	6	4	5	5	5	4
Knowledge of cyber threats and vulnerabilities.	6	4	4	5	3	5
Knowledge of cybersecurity and privacy principles.	6	7	7	2	3	5
Knowledge of information security program management and project management principles and techniques.	6	7	6	4	4	3
Knowledge of security management.	6	6	5	4	5	6
Knowledge of what constitutes a threat to a network.	6	4	5	3	4	5
Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	5	6	7	2	2	2
Knowledge of organizational security policies.	5	7	7	5	5	5
Knowledge of organization's risk tolerance and/or risk management approach.	5	3	5	4	4	5
Knowledge of risk/threat assessment.	5	5	3	4	3	5
Knowledge and understanding of operational design.	2	2	2	2	3	1

Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	1	0	1	0	0	0
Knowledge of information technology (IT) risk management policies, requirements, and procedures.	1	1	1	0	1	0
Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.	1	1	1	1	0	0
Knowledge of Risk Management Framework (RMF) requirements.	1	1	1	1	1	2

Learning Objective ECONOMICS & BUSINESS - Skills Row Labels	Sum of telecom	Sum of eHealth	Sum of finance	Sum of defense	Sum of transport	Sum of general
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	8	6	5	5	4	5
Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	6	5	5	3	4	6
Skill to anticipate new security threats.	6	4	7	5	5	6
Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	5	6	6	3	2	6
Skill in creating policies that reflect system security objectives.	5	5	6	4	3	6
Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	5	5	6	5	4	4
Skill in performing impact/risk assessments.	5	5	6	2	4	6
Skill in writing about facts and ideas in a clear, convincing, and organized manner.	5	4	4	4	3	8
Skill to use critical thinking to analyze organizational patterns and relationships.	4	3	6	2	5	8
Skill in translating operational requirements into protection needs (i.e., security controls).	3	4	3	2	3	3
Skill in talking to others to convey information effectively.	2	1	2	2	2	3

Annex 5: Scoring of top 10 Knowledge and Skills per Learning Objective – Telecom Industry

Knowledge	Threats	Technology	Economics
Knowledge and understanding of operational design.	4	6	2
Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	3	7	1
Knowledge of adversarial tactics, techniques, and procedures.	6	0	0
Knowledge of an organization's threat environment.	7	0	7
Knowledge of applicable business processes and operations of customer organizations.	0	0	7
Knowledge of applicable business processes and operations of customer organizations.	0	0	7
Knowledge of authentication, authorization, and access control methods.	6	0	0
Knowledge of computer networking concepts and protocols, and network security methodologies.	2	0	0
Knowledge of confidentiality, integrity, and availability principles.	6	4	6
Knowledge of confidentiality, integrity, and availability requirements.	7	5	7
Knowledge of countermeasure design for identified security risks.	0	6	0
Knowledge of current and emerging cyber technologies.	0	6	0
Knowledge of current and emerging threats/threat vectors.	4	0	0
Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	7	0	6
Knowledge of cyber defense and information security policies, procedures, and regulations.	6	0	7
Knowledge of cyber defense and vulnerability assessment tools and their capabilities.	0	1	0

Knowledge of cyber threats and vulnerabilities.	8	6	6
Knowledge of cybersecurity and privacy principles and methods that apply to software development.	0	6	0
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	6	0	7
Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	8	0	0
Knowledge of cybersecurity and privacy principles.	7	6	6
Knowledge of defense-in-depth principles and network security architecture.	8	7	0
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	6	0	0
Knowledge of emerging security issues, risks, and vulnerabilities.	6	0	0
Knowledge of industry standard security models.	0	1	0
Knowledge of industry technologies' potential cybersecurity vulnerabilities.	0	2	0
Knowledge of information security program management and project management principles and techniques.	0	0	6
Knowledge of information security systems engineering principles (NIST SP 800-160).	0	4	0
Knowledge of information technology (IT) architectural concepts and frameworks.	0	6	0
Knowledge of information technology (IT) risk management policies, requirements, and procedures.	4	5	1
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	0	1	0
Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	0	6	0
Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	0	0	7
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	0	0	7
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	5	9	0

Knowledge of organization's risk tolerance and/or risk management approach.	0	0	5
Knowledge of organizational security policies.	0	0	5
Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.	0	0	1
Knowledge of Risk Management Framework (RMF) requirements.	1	0	1
Knowledge of risk/threat assessment.	7	0	5
Knowledge of security management.	5	6	6
Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	0	8	0
Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	4	0	0
Knowledge of what constitutes a threat to a network.	6	0	6
Knowledge that technology that can be exploited.	3	5	0

Skills	Threats	Technology	Economics
Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	0	0	6
Skill in applying confidentiality, integrity, and availability principles.	11	7	0
Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	12	6	0
Skill in assessing security systems designs.	12	5	0
Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	9	4	5
Skill in creating policies that reflect system security objectives.	10	5	5
Skill in designing countermeasures to identified security risks.	11	5	0
Skill in designing multi-level security/cross domain solutions.	0	1	0
Skill in designing security controls based on cybersecurity principles and tenets.	0	2	0
Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	8	5	5
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	0	2	8

Skill in evaluating the adequacy of security designs.	9	5	0
Skill in performing impact/risk assessments.	10	5	5
Skill in talking to others to convey information effectively.	0	0	2
Skill in translating operational requirements into protection needs (i.e., security controls).	0	0	3
Skill in writing about facts and ideas in a clear, convincing, and organized manner.	0	0	5
Skill to anticipate new security threats.	11	0	6
Skill to use critical thinking to analyze organizational patterns and relationships.	0	0	4