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

Cyber security cOmpeteNCe fOr Research anD InnovAtion [†]

Work Package 5: Exploitation, Dissemination, Certification, and Standardization

C^3 by CONCORDIA – Certification Scheme

Abstract: This document contains the principles that the C^3 by CONCORDIA – Certification Scheme follows and relevant supporting information regarding the different processes implemented as part of the Scheme.

Contractual Date of Delivery	-
Actual Date of Delivery	*30/07/2021*
Deliverable Dissemination Level	*Public*
Editors	*Chatzopoulou Argyro*
Contributors	*TÜV TRUST IT, EIT DIGITAL, MU, UMIL, ARTHUR'S LEGAL, UL*
Quality Assurance	

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

The CONCORDIA Consortium

UniBW/CODE	University Bundeswehr Munich / Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JACOBSUNI	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
~~TUDA~~	~~Technical University of Darmstadt~~	~~Germany~~
MU	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
Imperial	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR ASA	Telenor ASA	Norway
AirbusCS-GE	Airbus Cybersecurity GmbH	Germany
SECUNET	secunet Security Networks AG	Germany
IFAG	Infineon Technologies AG	Germany
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
SURFnet bv	SURFnet bv	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG	RUAG AG (as a replacement for RUAG Schweiz AG)	Switzerland
BITDEFENDER	Bitdefender SRL	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens AG	Germany
Flowmon	Flowmon Networks AS	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia SPA	Italy
Efacec	EFACEC Electric Mobility SA (as a replacement for EFACEC Energia)	Portugal
ARTHUR'S LEGAL	Arthur's Legal B.V.	Netherlands
eesy-inno	eesy-innovation GmbH	Germany
DFN-CERT	DFN-CERT Services GmbH	Germany
CAIXABANK SA	CaixaBank SA	Spain
~~BMW Group~~	~~Bayerische Motoren Werke AG~~	~~Germany~~

GSDP	Ministry of Digital Policy, Telecommunications and Media	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia
UiO	University of Oslo	Norway
ULANC	University of Lancaster	UK
ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany
CRF	Centro Ricerche Fiat	Italy
ELTE	EOTVOS LORAND TUDOMANYEGYETEM	Hungary
Utimaco	Utimaco Management GmbH	Germany

Document Revisions & Quality Assurance

Internal Reviewers

Revisions:

Ver.	Date	By	Overview
1.0	*08.11.2021*	*Chatzopoulou Argyro*	*Initial Version*

Terms and definitions

Certification scheme for persons

competence and other requirements related to specific occupational or skilled categories of persons (ISO/IEC 17024 and ISO/IEC 17027). *For example there are schemes for the certification of "Food Auditors", "Welders" and "Cyber Security Specialists."*

Scheme owner

organization responsible for developing and maintaining a certification scheme.

NOTE: The organization can be the certification body itself, a governmental authority, or other. (ISO/IEC 17024 and ISO/IEC 17027)

Scope of certification

range and nature of specific tasks that a certified person is expected to be able to perform competently, by virtue of holding a specific certification that is within a certification scheme (ISO/IEC 17027).

Scope of certification scheme

extent and boundaries of a certification scheme (ISO/IEC 17027)

Interested party

individual, group or organization affected by the performance of a certified person or the certification body (ISO/IEC 17024 and ISO/IEC 17027)

Qualification

demonstrated education, training and work experience, where applicable (ISO/IEC 17024 and ISO/IEC 17027). Examples of qualifications include successful completion of a training or apprenticeship programme or *a university diploma. (*ISO/IEC 17024)

Certification process

activities by which a certification body determines that a person fulfils certification requirements, including application, assessment, decision on certification, recertification and use of certificates and logos/marks *(*ISO/IEC 17024)

Certification requirements

set of specified requirements, including requirements of the scheme to be fulfilled in order to establish or maintain certification. *(*ISO/IEC 17024)

Competence

ability to apply knowledge and skills to achieve intended results. *(*ISO/IEC 17024)

Assessment

process that evaluates a person's fulfilment of the requirements of the certification scheme. (ISO/IEC 17024)

Examination

mechanism that is part of the assessment which measures a candidate's competence by one or more means, such as written, oral, practical and observational, as defined in the certification scheme. (ISO/IEC 17024)

Examiner

person competent to conduct and score an examination, where the examination requires professional judgement. (ISO/IEC 17024)

Applicant

person who has submitted an application to be admitted into the certification process. (ISO/IEC 17024)

Candidate

applicant who has fulfilled specified prerequisites and has been admitted to the certification process. (ISO/IEC 17024)

Surveillance

periodic monitoring, during the periods of certification, of a certified person's performance to ensure continued compliance with the certification scheme. (ISO/IEC 17024)

e-CF

European e-Competence Framework (e-CF). The European e-Competence Framework provides a common language to describe the competences including skills and knowledge requirements of ICT professionals, professions and organisations at five proficiency levels, and is designed to meet the needs of individuals, businesses and other organisations in public and private sectors.[1]

[1] https://itprofessionalism.org/about-it-professionalism/competences/the-e-competence-framework/

Table of Contents

1 Introduction

Certification of persons provides assurance that the certified person meets the requirements of the certification scheme for persons, according to which certification was granted. Professional certifications that identify work related competencies and verify those individuals that can demonstrate that these competencies have been attained contributes to the development of human capital. In many countries evidence of qualification to perform a job is defined by the level and type of education or experience that person has acquired. However, there is often no formal link between a person's education or experience and the knowledge and skills needed to perform a job successfully. Sometimes when education is the only requirement for a job, employers complain that despite having the requisite education, workers are unable to competently perform a job. (UNITED NATIONS INDUSTRIAL DEVELOPMENT ORGANIZATION, 2016)

The work performed within Task T3.4 (Establishing an European Education Ecosystem for Cybersecurity) with the contribution of the outcomes / efforts of tasks T5.3 (Certification and Standardization activities), T4.1 (Working groups in technology domains of interest) and T4.3 (Economic perspectives), (CONCORDIA, 2020) showed that "Certification of Cybersecurity skills is a subject that professionals are pursuing in order to advance their careers or to retain their position" and "Employers have identified Certification of Cybersecurity skills as a useful tool in the validation of related skills.". Further research revealed the following gaps:

- There is a need for a Role profile definition for the Cybersecurity Consultant.
- There is a need for the creation of a suitable and reliable certification scheme for the Cybersecurity Consultant.

Previous efforts, (CONCORDIA, 2020) and (CONCORDIA, 2020), have provided a concrete Role Profile for the Cybersecurity Consultant. The produced profile contains the competencies that a person should have in order to effectively embody the role of the Cybersecurity Consultant.

This document describes the content of the C^3 by CONCORDIA (Cybersecurity Consultant certification scheme), including the practical methodology and details required to perform conformity assessment on the subject. This document identifies applicable requirements from other documents for the various components (e.g. requirements, requirements for certification, and markings etc).

2 The Certification Scheme for the Cybersecurity Consultant

2.1 Structure

The certification scheme for the Cybersecurity Consultant described within this document contains the following elements:

1. Scope of certification
2. Job and task description
3. Required competence
4. Abilities
5. Prerequisites

6. Declaration of Honor
7. Criteria for initial certification and recertification
8. Assessment methods for initial certification and recertification
9. Surveillance methods and criteria
10. Criteria for suspending and withdrawing certification
11. Storing and validating certificate information
12. Objections, complaints, appeals

The contents and processes described within this document, follow the international best practices of ISO/IEC 17024:2012 Conformity Assessment — General Requirements For Bodies Operating Certification Of Persons.

2.2 Scope of certification

The scope of a certification scheme is the description of the range and boundaries that apply. It informs the certified person and other interested parties of the nature and limits of the certification.

This certification scheme covers the following:

Job title: Cybersecurity Consultant

Certification title: Certified Cybersecurity Consultant – C^3 by CONCORDIA

Description of the Role's 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.

For the time being, the owner of the Certified Cybersecurity Consultant – C^3 by CONCORDIA is the CONCORDIA project. Since the CONCORDIA project is an EU-Funded project with a period of validity of 4 years (2019-2023), relevant activities will be undertaken before the end of the project to assign a new owner.

2.3 Job and task description

Every job is made up of a number of different tasks. A task is a job related activity. A certification scheme contains a description of the tasks required to perform the job.

The processes described in (CONCORDIA, 2020)[1] and (CONCORDIA, 2020) have derived a list of tasks that the Cybersecurity Consultant will be required to perform.

The list of these tasks based on the NICE framework is provided in Annex A. The number of tasks contained in this table is 163 and are judged to be too numerous to manage.

This is why, through the interpretation of the Profile to the e-cf, a grouping of tasks was able to be performed and the following list be derived.

[1] https://www.concordia-h2020.eu/wp-content/uploads/2020/07/CONCORDIAWorkshoponEducation2020-forpublication.pdf

Table 1. List of Tasks of the Cybersecurity Consultant based on the e-cf

Description of the Task
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 and assess relevant practices that evaluate compliance
Maintain current knowledge on relevant cybersecurity subjects and trends
Identify security requirements
Correct deficiencies
Conduct Risk Assessment

2.4 Required competence

After the tasks have been defined for a specific job, the knowledge and skills are identified. Competence is the ability to apply the knowledge and skills to achieve the intended results (to perform the tasks competently). A certification scheme for persons contains a way to verify the knowledge and skills required to perform the job effectively.

The processes described in (CONCORDIA, 2020) and (CONCORDIA, 2020) have derived a list of Knowledge and Skills that the Cybersecurity Consultant should have.

The list of these Knowledge and Skills based on the NICE framework is provided in Annex B. The number of Knowledge and Skills contained in this table are 86 and 38 respectively.

The interpretation of the Profile to the e-cf has provided the following table of competencies that the person should have. It is interesting to note that there are some competences that the Cybersecurity Consultant will be required to have that are not mapped to the e-CF competences.

For example: legal aspects, communication, project management etc. This stems from the fact that consulting is not a purely technical role. On the other hand, the e-CF contains only e-competences whereas the subjects mentioned above belong to a more generic category of competencies (a list of such competencies can be found on the ESCO website under the Skills/competences pillar)[1].

1 https://ec.europa.eu/esco/portal/skill?resetLanguage=true&newLanguage=en&skillFilterIndex=0#

Table 2. List of Competencies of the Cybersecurity Consultant based on the e-cf

Dimension 1 e-CF area	Dimension 2 e-competence	Dimension 3 e-competence proficiency level
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

The e-competencies mentioned above in Table 2, are further analyzed in EN 16234-1:2019, and a more detailed list of the competencies is provided. Due to the number of the e-competencies and also IPR considerations, the full information can not be included here. An analysis of one the e-competencies (A5. Architecture Design) is provided in Annex C.

2.5 Abilities

Based on the ISO CASCO guidance document (ISO, 2019), “Abilities are natural talents and aptitudes. Abilities can include physical capabilities such as vision, hearing and mobility.”

The Cybersecurity Consultant requires only vision as a physical capability. It should be noted that vision could be – to a degree – substituted or supported by accessibility tools that would allow for the person to gather the necessary information to perform the relevant tasks. (Example of such cases would be the review of log files, the configuration files of hardware, the status of equipment, etc).

In terms of Abilities as defined by the NICE framework, 34 Abilities have been identified as important for the Role of the Cybersecurity Consultant. These abilities are included in the Annex D.

2.6 Prerequisites

Prerequisites are the qualifications or competence required by a certification scheme for persons before one can be certified. When prerequisites are part of the certification scheme for persons they must be related to the competence requirements.

The CONCORDIA team has identified the following as minimum pre-requisites for the Certification Scheme of the Cybersecurity Consultant.

- 3 years of practical experience in the subject of Cybersecurity (Including but not limited to Cybersecurity Consulting, Cybersecurity Management etc) or a relevant Post -graduate Academic Degree.
- Successful attendance of a related theoretical training covering the basic knowledge mentioned above.*
- Successful attendance of a related practical – hands on training covering the practical skills mentioned above.*
- Basic knowledge of data structures and algorithmic principles, regular expressions, database principles, shell scription, networking principles, tools and architectures, operating systems basics, security controls, mechanisms and practice and risk management theories and methods is required.

* At this moment the only relevant course is the one offered by CONCORDIA[1]. After the scheme concludes its pilot operation, other relevant courses will be identified and the relevant descriptions will be updated.

[Note: When the scheme includes specific qualifications as prerequisites for a candidate, such as knowledge level, physical capability level, participation in a training program, etc, these must be clear, documented and publicly available in the frame that certification shall not be restricted on the grounds of any limiting conditions. Successful completion of an approved training program may be a prerequisite of a certification scheme, but the recognition / approval of a training program shall not compromise impartiality or reduce the assessment and certification requirements. (GUIDANCE FOR THE DEVELOPMENT AND RECOGNITION OF CERTIFICATION SCHEMES FOR PERSONS CONFORMITY WITH ELOT EN ISO/IEC 17024 REQUIREMENTS, 2013)]

2.7 Declaration of Honor

A declaration of Honor is a statement of expected behaviors of the certified person. It contains a description of professional, ethical or behavioral norms.

The practice of Cybersecurity related tasks and the handling of related information, could cause harm to individuals and organizations. This is why a declaration of Honor for the Cybersecurity Consultant has been created and is contained in Annex E.

2.8 Criteria for initial certification and recertification

A certification scheme for persons must include the criteria for both initial certification and recertification.

Examples of criteria for initial certification might include prerequisites or assessment/examination, or any other requirements for issuance of certifications (e.g. background checks).

Examples of criteria for recertification might include:

- On site assessment
- Professional development
- Structured interview
- Confirmation of continuing satisfactory work and work experience records
- Examination

[1] https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/

- Checks on physical capability.

The initial certification and recertification will be based on a successful computer-based assessment.

More information on the assessment method selected can be found in the following section 2.9.

2.8.1 Examination Committee/ Examiners

An Examination Committee has been formed, which consists of experts of CONCORDIA partners as examiners. All members of the Committee hold a university degree in a relevant to the examination subject sector and a specialization (either through further education and training or through professional experience) on the subject of Cybersecurity. The Committee's members are responsible for the preparation, the organizing, the implementation, the coordination and the supervision of the examinations. More specifically, they are responsible to ensure the smooth and secure operation of the examination procedure and the integrity of the examination result, to select the examination subjects depending on the scheme and the examination mechanism, to invigilate the candidates during the examination (if required), to assess and decide on the examination result (positive or negative), to complete the required documents of the scheme for the completion of the examination procedure, to publicize the examination results, to suggest the award or the maintenance or the change of the certificate to the scheme owner etc.

The members of the Examination Committee are selected and documented in the document, C^3 by CONCORDIA Examination Committe. The Examination Committee for the pilot exam was determined in March 2021 and will remain the same also for the next iteration of the exams. If needed, changes will be implemented and a record of these changes will be retained.

Before each examination, the names of the participants are shared with the Examination Committee in order to make sure that no conflicts of interest exist. If there are any conflicts of interest (e.g. there is a personal relation to the candidates or the examiner has provided related training activities, then that member of the Examination Committee will be excluded from the specific examination and another member will be selected to replace them.) (Note: For practical reasons this specific requirement has been waived for the pilot implementations of the scheme).

2.8.2 Requirements for the Certificate

All certification scheme's requirements must be satisfied in order to issue and award a certificate to a professional. After the Examination Committee's recommendation, the control of the examination evidence and the decision that all criteria for initial certification of the professional are met, the CONCORDIA project issues a certificate of conformity which has a unique registration number, the property of which remains with CONCORDIA project for the whole time of validity and until it is, in any way, suspended or withdrawn.

The form used for the certificates is designed in a way that minimizes the possibility for falsification and/or copying.

The form of the certificate includes the following information:

- Name and surname of the certified professional
- Unique code
- Name and logo of the CONCORDIA project
- The specialty of the certification scheme - Certified Cybersecurity Consultant – C3 by CONCORDIA
- Date of issue and date of end of validity of the certification

The information of the certificate is stored in the EduCTX [1] based on blockchain technology. EduCTX is a platform for managing students' micro-credentials (i.e., certificates), which is a solution already proven in pilot based-environment established among multiple academic institutions (e.g,. University of Maribor, University of Applied Sciences Bielefeld, University of Sarajevo and soon Brno University of Technology). This system allows for the easy and reliable validation and storage of a given certificate.

2.9 Assessment methods for initial certification and recertification

The assessment methods selected for initial certification are dependent on the scheme competence requirements. Assessment methods can include written, oral, practical or observational examinations. For example, if the scheme competence requirements include assessing keyboarding speed, then a practical examination might be used.

The certification scheme for persons can also specify the depth, length and content of the examination. By depth it is meant the degree of detail of knowledge and skills. By length it is meant the length of the examination in terms of number of questions or the time allowed to take the examination. By content it is meant the percentage of an examination devoted to each subject area.

To determine the compliance of a candidate with certification requirements, there must be at least one type of examination, during which evidence is collected, in order to measure a candidate's competence and lead to an impartial judgment. These could be simulation or real time tests, written exams, group or individual tasks, role-playing techniques (RP), etc.

Examination systems must be based on three main principles, during both their development and maintenance:

A) Validity. In order to be valid, examinations must assess these and only these that the scheme requires and collected evidence must demonstrate that the criteria are fulfilled. A candidate's performance must cover a sufficient range of knowledge and skills (competence), related to the scope of certification. Examination conditions must simulate adequately actual working conditions.

B) Reliability. There must be a univocal correlation between interpretation / recognition of a candidate's produced evidence and examination result. Scoring techniques must be clear and predefined. The comparability of results of each single examination must be ensured, regardless of examination time, examination sites, examination content and examiners conducting the examination. At this point, examiners play an important role, specifically their competence, experience, knowledge, personal characteristics and level of skills.

[1] https://eductx.org/

C) Fairness. Examinations must not favor any candidate over others. There must be no conflicts of interest e.g. personal or professional relationships, financial or other pressures, etc.

Based on the CONCORDIA Cybersecurity Skills Certification Framework and the Skills, Knowledge, Abilities and Tasks of the Role Profile of the Cybersecurity Consultant, the initial certification and recertification will be based on a successful computer based assessment.

More specifically, there will be an examination, administered through a suitable online system, comprising of two sections.

2.9.1 Section A. : Assessment method Theoretical method, written.

This section of the assessment aims to determine the existing theoretical knowledge of the candidate on topics linked to

(1) cybersecurity threats,
(2) novel technologies potentially bringing cybersecurity risks and
(3) economic perspectives linked to cybersecurity,

and will be grouped in the following areas.

- Cybersecurity principles
- Cybersecurity offensive methods
- Cybersecurity defensive methods
- Cybersecurity risk management

Section A will be run on a specialized platform benefiting from a proctoring feature. It contains questions (randomly selected from the relevant databank) to be answered through a selection from multiple choices of answers. Each candidate has to achieve a score of at least 70% on the Section A assessment in order to be allowed to participate in the Section B assessment. The questions for Section A, are included in a specifically constructed databank following the rules and guidelines mentioned below.

The basic principles adhered by all questions are the following:

- The questions are clear and concise.
- The type of answers will be multiple choice – between a selection of four answers.
- Each question has only one assigned difficulty level (Easy – Normal – Advanced).
- For each learning objective identified the databank includes questions from all difficulty levels following at least the percentage of selection (30% - 50% - 20% respectively).
- The total number of questions per examination will be 50.
- A candidate will need to score of 70% or more in order to pass this section of the exam.
- A candidate will need to score of 60% or more per Learning Objective in order to pass this section of the exam.
- Each question is awarded one mark. No negative marking is applicable.

- Before each examination, the examination Committee, will run a random process for the selection of 50 questions from all levels of difficulty with the following distribution 30%, 50% and 20% respectively.
- All learning objectives will be equally covered.
- The questions will be implemented in the online examination system and the results will be automatically extracted through the system. A review of the question databank will be implemented once a year by the committee and new questions will be added based on the exam statistics.

After each exam, the examination committee will check a sample of the exams in order to make sure that no mistake has occurred.

2.9.2 Section B. : Assessment method Practical method, simulation

This section of the assessment aims to determine the existing practical knowledge of the candidate on the following areas.

- Risk assessment
- Threat identification
- Vulnerabilities
- Source code analysis
- Penetration testing
- Cybersecurity Economics

And validate the following abilities of the Role Profile (based on NIST):

- **A0001** Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
- **A0015** Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
- **A0033** Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.
- **A0048** Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- **A0052** Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
- **A0055** Ability to operate common network tools (e.g., ping, traceroute, nslookup).
- **A0058** Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).
- **A0062** Ability to monitor measures or indicators of system performance and availability.
- **A0064** Ability to interpret and translate customer requirements into operational capabilities.
- **A0085** Ability to exercise judgment when policies are not well-defined.
- **A0092** Ability to identify/describe target vulnerability.
- **A0093** Ability to identify/describe techniques/methods for conducting technical exploitation of the target.
- **A0094** Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.
- **A0095** Ability to interpret and translate customer requirements into operational action.
- **A0096** Ability to interpret and understand complex and rapidly evolving concepts.

- **A0106** Ability to think critically.

Section B comprises of scenarios implemented through a cyberrange. The system provides a simulation of a real life situation and aims to the assessment and validation of the practical skills of the candidate in the above mentioned areas.

Before each examination, the examination Committee, will run a random process for the selection of the one scenario that will be implemented for a given exam.

Each candidate has to achieve a score of at least 80% in order to successfully complete the Section B assessment.

Candidates fulfilling all the criteria regarding the pre-requisites and all sections of the assessment as mentioned above are eligible for certification (initial or re-certification).

2.10 Surveillance methods and criteria

Surveillance is the periodic monitoring of a certified person's performance between certification and recertification to ensure continued compliance with the certification scheme. To determine the need for surveillance the scheme owner takes into consideration factors such as changing technology, length of recertification cycle, risk and consequences of incompetence.

Technology related to Cybersecurity as well as the methods of attacks, continually evolve, so Cybersecurity Professionals need to maintain their knowledge, skills and abilities as current as possible.

The CONCORDIA team, has decided to mandate a CPE requirement as means to make sure that the Cybersecurity Consultant continues to have updated knowledge and skills throughout the duration of the certificate.

Continuing professional education, or CPE, credit is a term referring to the points professionals receive for participating in specialized training in IT and other fields. CPE credits are based on hours of study and count toward certification programs that enable professionals to maintain or update their credentials.[1]

Specifically, every C^3 by CONCORDIA (Cybersecurity Consultant) certificate holder, during the three year period of validity of the certificate, has to collect a minimum of 90 CPEs.

CPEs can be collected through activities like:

- Publishing a cybersecurity related book, white paper or article.
- Attending a cybersecurity related conference.
- Taking an educational course, seminar or presentation, preparing for a presentation or teaching information related to cybersecurity.
- Cybersecurity related self-study related to research for a project, preparing for a related certification examination.

[1] https://whatis.techtarget.com/definition/CPE-credit

- Taking a cybersecurity related higher academic course.
- Attending a cybersecurity related educational course, seminar or presentation.
- Preparing for a cybersecurity related presentation or teaching information related to cybersecurity related.

For each hour of implementation of the above mentioned activities, 1 CPE is collected. The C^3 by CONCORDIA (Cybersecurity Consultant) certificate holder shall retain documented information as evidence of compliance to the CPE requirement. The CPEs are reported in the relevant system of the certification scheme owner and an audit could be carried out by the certification scheme owner to ensure compliance and integrity. (Note: For the pilot runs of the certification scheme this requirement has been waived).

2.11 Criteria for suspending and withdrawing certification

The criteria for suspending or withdrawing the certification are included in the certification scheme for persons. Examples of conditions under which the certification can be suspended or withdrawn are a violation of the Declaration of Honor, failure to comply with the scheme requirements, unsatisfactory surveillance results or inability to continually fulfil the competence requirements of the scheme.

Scheme owner has the right to suspend the Certificate of a professional, in case there is an objective proof that the professional has not complied with the relevant commitments and with the Declaration of Honor.

Indicative cases that might lead to the suspension (and then to the withdrawal) of a certificate are:

- receiving of a complaint or an appeal by a consumer about a specific professional, certificate's use in a way that harms the Scheme owner's reliability,
- receiving of a complaint about his professional competence by a consumer or an employer or another interested party,
- certificate's use in a misleading or fraudulent manner and for other levels/ categories from those that the professional has been certified for,
- inability of the certified professional to apply the terms and conditions for the maintenance of the certification,

In case of a complaint, a committee is created and an investigation is carried out. Based on the results the relevant activities are carried out by the Scheme owner.

The certified professional is informed in written for the identified problems. In case the problems are not solved within a short time, then the Certificate is suspended for six months.

If after the six months period, the problems have still not been solved, then the Scheme owner withdraws the Certificate. In case of a withdrawal, the professional has no longer the right to participate to another examination of this Scheme.

Otherwise, the suspension is lifted and the Certificate becomes valid again.
(The application for certification includes a term about the applicant's commitment to stop

any misleading use of the certification and/or the certificate, in case it is suspended or withdrawn.)

2.12 Storing and Validating certificate information

The information regarding the certification process (from Application to Certificate Maintenance) has to be retained by the Scheme owner for at least 6 years for each issued certificate. The Scheme owner will implement measures to assure the integrity, confidentiality and availability of the related information.

An interested party or the certificate holder can request to validate the information of the certificate.

For the storing of the C^3 by CONCORDIA certificates, a blockchain based solution is utilized, allowing for the seamless validation and storage of the certificate information.

The C^3 by CONCORDIA certificate is issued under the blockchain based platform EduCTX, developed and managed by University of Maribor. The certificate contains, amongst others, information regarding the date of issuing and expiration, the conditions of validity and security elements for easy identification.

2.12.1 Additional information on the usage of Blockchain

The usage of the Blockchain technology for cybersecurity certificates in the present case will abide to the three pillars of the technology, namely:

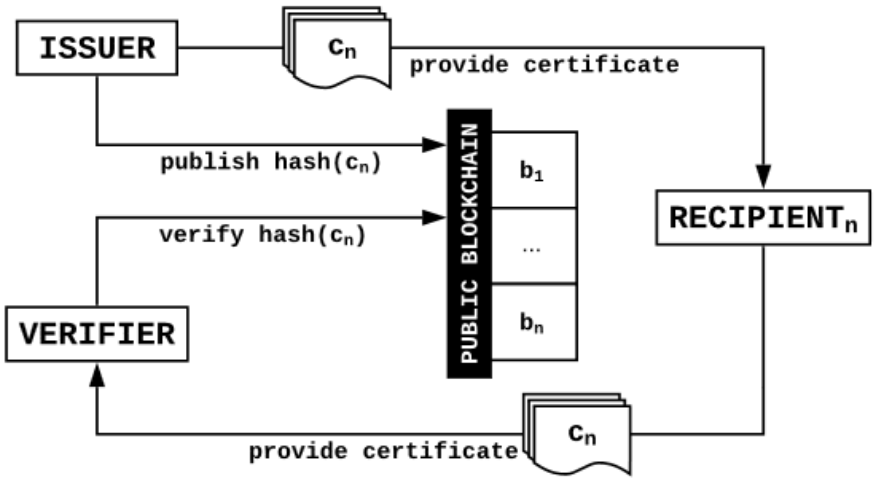
- Decentralization
- Transparency
- Immutability

The very interesting aspect of the technology is that it‘s shared and immutable ledger is open for anyone and everyone to see. It operates on time-stamped series record of data that is distributed and managed by a cluster of computers. The blockchain concept will be used to manage the certificate delivered by the Scheme owner and is accessible by any person, the candidate and other interested parties alike.

As indicated in the table below, only Issuers should be able to write authenticated hashes. Only European cybersecurity educational institutions (e.g., CONCORDIA partners) should be allowed to issue diplomas or certificates. Consequently, Recipients and Verifiers must only be able to read from the blockchain, allowing them to verify the certificate.

Stakeholder	Read	Write
Issuer	✔	✔
Recipient	✔	✘
Verifier	✔	✘
Endorser	✔	✘

And the high level workflow is the one depicted below



Annex A -List of Tasks of the Cybersecurity Consultant based on the NICE framework

T - ID	Description of Tasks
T0010	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
T0018	Assess the effectiveness of cybersecurity measures utilized by system(s).
T0019	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.
T0075	Provide technical summary of findings in accordance with established reporting procedures.
T0097	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.
T0102	Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.
T0119	Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements.
T0133	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.
T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.
T0177	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
T0178	Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.
T0231	Provide support to security/certification test and evaluation activities.
T0244	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.
T0263	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.
T0291	Examine network topologies to understand data flows through the network.
T0309	Assess the effectiveness of security controls.
T0327	Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.
T0328	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.
T0372	Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.

T - ID	Description of Tasks
T0400	Correlate incident data and perform cyber defense reporting.
T0410	Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities.
T0425	Analyze organizational cyber policy.
T0433	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.
T0470	Analyze and report system security posture trends.
T0475	Assess adequate access controls based on principles of least privilege and need-to-know.
T0504	Assess and monitor cybersecurity related to system implementation and testing practices.
T0505	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.
T0508	Verify minimum security requirements are in place for all applications.
T0518	Perform security reviews and identify security gaps in architecture.
T0538	Provide support to test and evaluation activities.
T0556	Assess and design security management functions as related to cyberspace.
T0577	Assess efficiency of existing information exchange and management systems.
T0589	Assist in the identification of intelligence collection shortfalls.
T0686	Identify threat vulnerabilities.
T0710	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.
T0724	Identify potential points of strength and vulnerability within a network.
T0845	Identify cyber threat tactics and methodologies.
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.
T0054	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
T0071	Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).
T0078	Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications.
T0082	Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.
T0106	Identify alternative information security strategies to address organizational security objective.

T - ID	Description of Tasks
T0115	Identify information technology (IT) security program implications of new technologies or technology upgrades.
T0143	Make recommendations based on test results.
T0187	Plan and recommend modifications or adjustments based on exercise results or system environment.
T0200	Provide feedback on network requirements, including network architecture and infrastructure.
T0202	Provide cybersecurity guidance to leadership.
T0219	Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.
T0227	Recommend policy and coordinate review and approval.
T0261	Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.
T0271	Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).
T0282	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.
T0348	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.
T0360	Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.
T0414	Develop supply chain, system, network, performance, and cybersecurity requirements.
T0446	Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.
T0449	Design to security requirements to ensure requirements are met for all systems and/or applications.
T0454	Define baseline security requirements in accordance with applicable guidelines.
T0472	Draft, staff, and publish cyber policy.
T0478	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.
T0484	Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.
T0526	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
T0527	Provide input to implementation plans and standard operating procedures as they relate to information systems security.
T0528	Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials
T0529	Provide policy guidance to cyber management, staff, and users.

T - ID	Description of Tasks
T0536	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).
T0537	Support the CIO in the formulation of cyber-related policies.
T0546	Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.
T0548	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.
T0550	Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).
T0551	Draft and publish supply chain security and risk management documents.
T0560	Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).
T0782	Provide analyses and support for effectiveness assessment.
T0875	Assist the Security Officer with the development and implementation of an information infrastructure
T0174	Perform needs analysis to determine opportunities for new and improved business process solutions.
T0208	Provide recommendations for possible improvements and upgrades.
T0708	Identify threat tactics, and methodologies.
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.
T0076	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.
T0158	Participate in an information security risk assessment during the Security Assessment and Authorization process.
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
T0199	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
T0214	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
T0233	Track and document cyber defense incidents from initial detection through final resolution.
T0273	Develop and document supply chain risks for critical system elements, as appropriate.
T0306	Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.

T - ID	Description of Tasks
T0308	Analyze incident data for emerging trends.
T0486	Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.
T0509	Perform an information security risk assessment.
T0533	Review, conduct, or participate in audits of cyber programs and projects.
T0549	Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).
T0928	Collaborate with key stakeholders to establish a cybersecurity risk management program.
T0041	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.
T0073	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.
T0142	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.
T0155	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.
T0188	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.
T0212	Provide technical assistance on digital evidence matters to appropriate personnel.
T0234	Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
T0248	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
T0251	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).
T0260	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.
T0307	Analyze candidate architectures, allocate security services, and select security mechanisms.
T0315	Develop and deliver technical training to educate others or meet customer needs.
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.
T0395	Write and publish after action reviews.
T0450	Design training curriculum and course content based on requirements.
T0451	Participate in development of training curriculum and course content.

T - ID	Description of Tasks
T0502	Monitor and report client-level computer system performance.
T0503	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
T0510	Coordinate incident response functions.
T0519	Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for the most effective learning environment.
T0530	Develop a trend analysis and impact report.
T0547	Research and evaluate available technologies and standards to meet customer requirements.
T0738	Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications.
T0834	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.
T0847	Maintain awareness of target communication tools, techniques, and the characteristics of target communication networks (e.g., capacity, functionality, paths, critical nodes) and their potential implications for targeting, collection, and analysis.
T0871	Collaborate on cyber privacy and security policies and procedures
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
T0017	Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.
T0074	Develop policy, programs, and guidelines for implementation.
T0123	Implement specific cybersecurity countermeasures for systems and/or applications.
T0159	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.
T0194	Properly document all systems security implementation, operations, and maintenance activities and update as necessary.
T0465	Develop guidelines for implementation.
T0485	Implement security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed.
T0489	Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.
T0297	Identify applications and operating systems of a network device based on network traffic.

T - ID	Description of Tasks
T0022	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.
T0060	Develop an understanding of the needs and requirements of information end-users.
T0061	Develop and direct system testing and validation procedures and documentation.
T0088	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.
T0090	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.
T0101	Evaluate the effectiveness and comprehensiveness of existing training programs.
T0105	Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements.
T0118	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.
T0121	Implement new system design procedures, test procedures, and quality standards.
T0127	Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements.
T0186	Plan, execute, and verify data redundancy and system recovery procedures.
T0203	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.
T0246	Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.
T0270	Analyze user needs and requirements to plan and conduct system security development.
T0272	Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.
T0274	Create auditable evidence of security measures.
T0284	Design and develop new tools/technologies as related to cybersecurity.
T0323	Develop or assist in the development of written tests for measuring and assessing learner proficiency.
T0388	Review and apply organizational policies related to or influencing the cyber workforce.
T0427	Analyze user needs and requirements to plan architecture.
T0453	Determine and develop leads and identify sources of information to identify and/or prosecute the responsible parties to an intrusion or other crimes.
T0467	Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness.

T - ID	Description of Tasks
T0483	Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).
T0496	Perform asset management/inventory of information technology (IT) resources.
T0499	Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.
T0535	Recommend revisions to curriculum and course content based on feedback from previous training sessions.
T0552	Review and approve a supply chain security/risk management policy.
T0718	Identify intelligence gaps and shortfalls.
T0835	Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date.

Annex B - List of Knowledge and Skills that a Cybersecurity Consultant should have based on the NICE framework

K - ID	Description of Knowledge
K0310	Knowledge of hacking methodologies.
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004	Knowledge of cybersecurity and privacy principles.
K0344	Knowledge of an organization's threat environment.
K0005	Knowledge of cyber threats and vulnerabilities.
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.
K0295	Knowledge of confidentiality, integrity, and availability principles.
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
K0211	Knowledge of confidentiality, integrity, and availability requirements.
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.
K0149	Knowledge of organization's risk tolerance and/or risk management approach.
K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0165	Knowledge of risk/threat assessment.
K0276	Knowledge of security management.
K0297	Knowledge of countermeasure design for identified security risks.
K0612	Knowledge of what constitutes a "threat" to a network.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
K0222	Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
K0151	Knowledge of current and emerging threats/threat vectors.
K0214	Knowledge of the Risk Management Framework Assessment Methodology.
K0335	Knowledge of current and emerging cyber technologies.
K0013	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.

K0048	Knowledge of Risk Management Framework (RMF) requirements.
K0007	Knowledge of authentication, authorization, and access control methods.
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
K0242	Knowledge of organizational security policies.
K0008	Knowledge of applicable business processes and operations of customer organizations.
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.
K0112	Knowledge of defense-in-depth principles and network security architecture.
K0119	Knowledge of hacking methodologies.
K0158	Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
K0299	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.
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0032	Knowledge of resiliency and redundancy.
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
K0115	Knowledge that technology that can be exploited.
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
K0234	Knowledge of full spectrum cyber capabilities (e.g., defense, attack, exploitation).
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.
K0110	Knowledge of adversarial tactics, techniques, and procedures.
K0121	Knowledge of information security program management and project management principles and techniques.
K0288	Knowledge of industry standard security models.
K0487	Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).
K0006	Knowledge of specific operational impacts of cybersecurity lapses.
K0009	Knowledge of application vulnerabilities.
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
K0347	Knowledge and understanding of operational design.
K0336	Knowledge of access authentication methods.
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).

K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.
K0160	Knowledge of the common attack vectors on the network layer.
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
K0042	Knowledge of incident response and handling methodologies.
K0499	Knowledge of operations security.
K0292	Knowledge of the operations and processes for incident, problem, and event management.
K0293	Knowledge of integrating the organization's goals and objectives into the architecture.
K0104	Knowledge of Virtual Private Network (VPN) security.
K0314	Knowledge of industry technologies' potential cybersecurity vulnerabilities.
K0613	Knowledge of who the organization's operational planners are, how and where they can be contacted, and what are their expectations.
K0231	Knowledge of crisis management protocols, processes, and techniques.
K0058	Knowledge of network traffic analysis methods.
K0047	Knowledge of information technology (IT) architectural concepts and frameworks.
K0066	Knowledge of Privacy Impact Assessments.
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.
K0342	Knowledge of penetration testing principles, tools, and techniques.
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.
K0088	Knowledge of systems administration concepts.
K0174	Knowledge of networking protocols.
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.
K0065	Knowledge of policy-based and risk adaptive access controls.
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0075	Knowledge of security system design tools, methods, and techniques.
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.
K0195	Knowledge of data classification standards and methodologies based on sensitivity and other risk factors.
K0240	Knowledge of multi-level security systems and cross domain solutions.

K0296	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.

S - ID	Description of Skills
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
S0006	Skill in applying confidentiality, integrity, and availability principles.
S0010	Skill in conducting capabilities and requirements analysis.
S0018	Skill in creating policies that reflect system security objectives.
S0022	Skill in designing countermeasures to identified security risks.
S0023	Skill in designing security controls based on cybersecurity principles and tenets.
S0027	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.
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
S0036	Skill in evaluating the adequacy of security designs.
S0070	Skill in talking to others to convey information effectively.
S0072	Skill in using scientific rules and methods to solve problems.
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
S0085	Skill in conducting audits or reviews of technical systems.
S0086	Skill in evaluating the trustworthiness of the supplier and/or product.
S0116	Skill in designing multi-level security/cross domain solutions.
S0134	Skill in conducting reviews of systems.
S0137	Skill in conducting application vulnerability assessments.
S0140	Skill in applying the systems engineering process.
S0141	Skill in assessing security systems designs.
S0145	Skill in integrating and applying policies that meet system security objectives.
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
S0152	Skill in translating operational requirements into protection needs (i.e., security controls).
S0171	Skill in performing impact/risk assessments.
S0175	Skill in performing root cause analysis.
S0177	Skill in analyzing a target's communication networks.
S0232	Skill in identifying intelligence gaps and limitations.
S0242	Skill in interpreting vulnerability scanner results to identify vulnerabilities.
S0244	Skill in managing client relationships, including determining client needs/requirements, managing client expectations, and demonstrating commitment to delivering quality results.
S0249	Skill in preparing and presenting briefings.
S0250	Skill in preparing plans and related correspondence.

S0273	Skill in reviewing and editing plans.
S0278	Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).
S0296	Skill in utilizing feedback to improve processes, products, and services.
S0301	Skill in writing about facts and ideas in a clear, convincing, and organized manner.
S0356	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).
S0357	Skill to anticipate new security threats.
S0358	Skill to remain aware of evolving technical infrastructures.
S0359	Skill to use critical thinking to analyze organizational patterns and relationships.

Annex C - Example of the details of the e-CF (2019) for A5. Architecture Design

A.5. Architecture Design	Level 5
Specifies, refined, updates and makes available a formal approach to implement solutions and services necessary to develop and operate the IS architecture, taking into account the requirements from business, management and data and information infrastructure. Identifies change requirements and the components involved: hardware, software, applications, processes, services, information and technology platform. Takes into account interoperability, reversibility, scalability, usability, accessibility and security, including the need to account for the development and management of vulnerability within existing and emerging technologies. Maintain alignment business evolution and technology development and services to ensure capacity of IT solutions according to SLA.	Provides strategic leadership for implementing the digital enterprise strategy. Applies strategic thinking to discover and recognize new patterns in data sets and new ICT systems, to achieve business benefits.
Knowledge examples	
K1 – architecture frameworks, methodologies and system design tools	
K2 – systems architecture requirements: performance, maintainability, extendibility, scalability, availability, security and accessibility	
K3 – costs, benefits and risks of a system architecture	
K4 – the company's enterprise architecture and its interconnection to networks	
K5 – new emerging technologies (e.g. distributed systems, cloud computing, virtualization models, datasets, mobile systems)	
K6 – principles and techniques for access management	
K7 – principles of systems and data security	
Skills examples	
S1 – provide expertise to help solve complex technical problems and ensure best architecture solutions are implemented	
S2 – use of knowledge in various technology areas to build and deliver the enterprise architecture	
S3 – understand the business objectives / drivers that impact the architecture component (data, application, security, development etc)	
S4 – apply security design principle e.g. least privilege	
S5 – assist in communication of the enterprise architecture and standards, principles and objectives to the application teams	
S6 – develop design patterns and models to assist system analysts in designing consistent applications	
S7 – build resilience against points of failure across the architecture	
S8 – assess and apply access control techniques	

Annex D - List of Abilities of the Cybersecurity Consultant based on the NICE framework

ID	Description
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
A0004	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.
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.
A0009	Ability to apply supply chain risk management standards.
A0011	Ability to answer questions in a clear and concise manner.
A0013	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
A0014	Ability to communicate effectively when writing.
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
A0018	Ability to prepare and present briefings.
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.
A0048	Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
A0052	Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
A0055	Ability to operate common network tools (e.g., ping, traceroute, nslookup).
A0057	Ability to tailor curriculum that speaks to the topic at the appropriate level for the target audience.
A0058	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).
A0062	Ability to monitor measures or indicators of system performance and availability.
A0064	Ability to interpret and translate customer requirements into operational capabilities.
A0070	Ability to apply critical reading/thinking skills.
A0074	Ability to collaborate effectively with others.
A0082	Ability to effectively collaborate via virtual teams.
A0083	Ability to evaluate information for reliability, validity, and relevance.
A0085	Ability to exercise judgment when policies are not well-defined.
A0088	Ability to function effectively in a dynamic, fast-paced environment.
A0092	Ability to identify/describe target vulnerability.
A0093	Ability to identify/describe techniques/methods for conducting technical exploitation of the target.
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.
A0095	Ability to interpret and translate customer requirements into operational action.
A0096	Ability to interpret and understand complex and rapidly evolving concepts.
A0106	Ability to think critically.
A0108	Ability to understand objectives and effects.

A0110	Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance.
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.

Annex E – Declaration of Honor

Declaration of Honor

WHY
As cybersecurity and related domains and dimensions are about ethical professionalism and related responsible and accountable behavior by each individual involved in these domains and dimension, all participants to the Cybersecurity Consultant Courses provided by CONCORDIA and candidates for the C^3 by CONCORDIA certification are invited – at their discretion and without legal obligation – to sign this Declaration of Honor.

DECLARATION
Therefor I hereby declare that do my best efforts to comply with any and all moral and social obligations and related accountability towards myself, customers, society and others that are associated with aiming to become, becoming, acting as, remaining and continuously improve as a Cybersecurity Consultant.

These moral obligations for once include (without limitation) the ability to make informed decisions, the ability to challenge and improve both before (by design), during and after initiatives, decisions, actions or omissions, and the ability to aim for no surprises for anybody (including deploying the principles of trust, transparency, confidentiality, integrity and accountability).

In this spirit and without prejudice to the applicable regulations and any professional Code of Ethics/Conduct I already have adhered to or intend to adhere to in the future, I aim to implement the knowledge and skills acquired during and related to the CONCORDIA Cybersecurity Consultant Courses.

Acknowledging the cybersecurity challenges people, organizations, society, member states, regions, the European Union and its friends and allies encounter in this Digital Age and as an integral part of my moral obligations, I further declare that I make all reasonable efforts to maintain the aforementioned knowledge and skills and to continuously develop them by participating in appropriate educational activities organized under the auspices of credible organizations and initiatives.

I acknowledge that any deviation from this Declaration of Honor may be considered as a form of professional misconduct with impact – also – the professional credibility of myself as well as the relevant teams and community I am part of.

Date & Signature

Bibliography

CONCORDIA. (2020). *CONCORDIA Workshop on Education for cybersecurity professionals post workshop report.* Brussels: CONCORDIA.

CONCORDIA. (2020). *Cybersecurity Consultant - Creating the Role Profile.* Brussels: CONCORDIA.

CONCORDIA. (2020). *Feasibility Study "Cybersecurity Skills Certification".* Brussels: CONCORDIA.

(2013). *GUIDANCE FOR THE DEVELOPMENT AND RECOGNITION OF CERTIFICATION SCHEMES FOR PERSONS CONFORMITY WITH ELOT EN ISO/IEC 17024 REQUIREMENTS.* Athens: Hellenic Accreditation System.

(2016). *How to develop schemes for the certification of persons - Guidance of ISO/IEC 17024.* Geneva: ISO Central Secretariat.

ISO. (2012). *ISO/IEC 17024:2012 - Conformity assessment — General requirements for bodies operating certification of persons.* Geneva: ISO.

ISO. (2014). *ISO/IEC TS 17027:2014 - Conformity Assessment - Vocabulary related to competence of persons used for certification of persons.* Geneva: ISO.

ISO. (2019). *How to develop scheme documents - Guidance for ISO technocal committees.* Geneva: ISO Central Secretariat.

UNITED NATIONS INDUSTRIAL DEVELOPMENT ORGANIZATION. (2016). *Guidelines on conformity assessment - ISO/IEC 17024:2012.* Vienna: UNITED NATIONS INDUSTRIAL DEVELOPMENT ORGANIZATION.