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*

CONCORDIA Cybersecurity Skills Certification Framework

Abstract: This document contains CONCORDIA's recommendation for a Cybersecurity Skills Certification Framework. The document is aligned to and provides further specification on the requirements of ISO/IEC 17024:2012 CONFORMITY ASSESSMENT — GENERAL REQUIREMENTS FOR BODIES OPERATING CERTIFICATION OF PERSONS

Date of Delivery	*20.09.2022*
Actual Date of Delivery	*Final*
Deliverable Dissemination Level	*Public*
Editors	*Chatzopoulou Argyro (TUV)*
Contributors	*Anisetti Marco (*UMIL) *Badonnel Remi (UL)* *Bena Nicola (*UMIL) *Carminati Barbara (UI)* *Cholez Thibault (UL)* *Cutas Felicia (EIT DIGITAL)* *Ferrari Elena (UI)* *Fournaris Apostolos (ISI)* *Franco Muriel (UZH)* *Prelipcean Dumitru Bogdan (BITDEFENDER)*

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

	Scheid Eder John (UZH) *Sleem Lama (UL)* *Van Der Wees Arthur (ARTHUR'S LEGAL)*
Quality Assurance	*Lampropoulos Kostas (UP)* *Tobeck Nils (AirbusCS-GE)*

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 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 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	Greece

	Media	
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

Disclaimer:
The sole responsibility of this document lies with the authors. The European Commission is not responsible for any use that may be made of the information contained therein.

Executive summary

As part of Task T3.4 - Establishing an European Education Ecosystem for Cybersecurity, the CONCORDIA project has implemented various activities in relation to cybersecurity skills training courses. (More information can be found at https://www.concordia-h2020.eu/concordia-service-cybersecurity-skills/). During these activities, a gap was identified in relation to the certification of the knowledge, skills and abilities of cybersecurity professionals. Specifically, although many certification schemes exist in the are of cybersecurity skills, there is no common approach and baseline leading to a fragmentation of the market and a reduction to the possible value of such certifications.

This document contains CONCORDIA's recommendation for a Cybersecurity Skills Certification Framework. The document is aligned to and provides further specification on the requirements of ISO/IEC 17024:2012 CONFORMITY ASSESSMENT — GENERAL REQUIREMENTS FOR BODIES OPERATING CERTIFICATION OF PERSONS.

It should be noted that not all of the requirements of ISO/IEC 17024:2012 are included in this document. It is envisaged that the certifying organization will follow all of the requirements of ISO/IEC 17024:2012 with the addition of the ones mentioned within this document, as specialization to the cybersecurity skills domain.

Contents

1. Introduction

With interconnectivity and internet changing at a very rapid speed, evolving threats and Cybersecurity is becoming a hot issue and no individual or organization with online presence can be spared from it. Besides, digitization of the whole economy (before, during and because of and after the world pandemic crisis) worsens the issue and also influences the labour market in terms of a higher demand.

There are several surveys conducted by Professional Organizations worldwide on the subject of Cybersecurity Skills, their current situation, the possible value of related certifications and the steps that need to be performed. The project team conducted a literature review, through which several of these surveys were analysed and their results evaluated. The sources, analysis and results of this review are contained in the document Feasibility Study "Cybersecurity Skills Certifications"[1]. The information within clearly shows that there is still a Cybersecurity Skills Gap.

1.1. Structure

This document is structured as follows:

Section 1, introduces the subject of the Cybersecurity Skills Gap and how a Cybersecurity Skills Certification Framework could help in addressing it.

Section 2, provides an overview of the terms and definitions needed to interpret this document and the predominant standard regarding the Certification of Persons (Skills Certification) and introduces the basic principles that should be applied based on this standard.

Section 3, adds to the principles that should be adopted with others needed especially for the Cybersecurity domain.

Section 4, provides the conclusions of this effort and envisioned next steps.

1.2. The Cybersecurity Skills Gap

At the time of the last revision of this document, the most recent publications in relation to the Cybersecurity Skills Gap are: STATE OF CYBERSECURITY 2021, PART 1: GLOBAL UPDATE ON WORKFORCE EFFORTS, RESOURCES AND BUDGETS, ISACA[2] and (ISC)2 Cybersecurity Workforce Study, 2021, (ISC)2[3].

The reports indicate that there is still a worldwide cybersecurity skills gap, although there have been several initiatives in the education and awareness area.

"The cybersecurity workforce shortage persists and likely will continue, until there is an honest analysis of what is and is not working. Despite years of effort by government, industry and academia, and despite the expenditure of large swaths of taxpayer dollars, little has changed." (ISACA)

[1] https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-SkillsFeasibilityStudy-forpublication.pdf

[2] https://www.isaca.org/go/state-of-cybersecurity-2021

[3] https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

At the same time Pathways to cybersecurity are changing. “While an IT background remains the single most common route taken (47% of participants), that is giving way to a variety of entry points. Slightly more than half of cybersecurity professionals got their start outside of IT—17% transitioned from unrelated career fields, 15% gained access through cybersecurity education and 15% explored cybersecurity concepts on their own”. (ISC2)

The above further increase the challenges of hiring managers and their organizations in selecting the most suitable candidate to effectively fill a job role. “Survey data extend previous reporting that hiring managers have low confidence in cybersecurity applicants.” (ISACA)

Certification of cybersecurity skills, is one of the possible solutions for the verification of the skills not just for the technical vendor oriented but also on the practical and soft skills related to cybersecurity. This is also supported by the survey data “According to the study, 72% of cybersecurity professionals are required by their organization to earn certifications, with the demand almost evenly split between vendor-neutral certifications such as the CISSP and CISM, and vendor-specific certificates, such as those issued by Cisco and Microsoft.” (ISACA)

Whereas some of Benefits of Employing Certified Professionals are pointed out “Study participants tell us certifications held by individuals create advantages and opportunities for the entire team and specifically, Stronger knowledge in key cybersecurity areas (38%), Increased confidence in the team’s handling of security challenges (30%), Higher-level personnel in-house with security expertise (27%), Staying up to date on the latest security and privacy trends (27%)”. (ISC2)

Taking these facts, and the value of Cybersecurity Skills Certification, the CONCORDIA Feasibility Study “Cybersecurity Skills Certifications” also showed that there is a huge variety of related Certification Schemes. The document identifies more than 60 related certification schemes that had already gained momentum at the time of the it’s drafting.

The fact that there is such a variety of Cybersecurity Skills certification schemes, burdens both the professional and the hiring managers and organizations.

1.3. A Cybersecurity Skills Certification Framework

The answer to the challenges and problems mentioned above, is more than just Certification. Specifically, ECSO in the publication “ECSO Information and Cyber Security Professional Certification v3”, last update 2020, notes that “ECSO should support ENISA and the European standardisation bodies in the development of one European-wide certification scheme and baseline requirements for certification schemes to be met under the purview of public procurement, cyber security and critical infrastructure regulation. As a result, ENISA (or other suitable European body) can offer a European accreditation scheme for cyber security certifications. Leveraging existing market offerings by creating an accreditation scheme for existing cyber security certifications for personnel on a European level, has the potential to drive harmonisation and quality assurance across the board without sacrificing the investment by professionals and businesses in existing certifications.[4]"

This means that there is a need for Certification of Cybersecurity Skills, but in a way that the resulting Certificate is a true testament of the skills of a professional, taking into consideration the specificities of the Cybersecurity domain and paving the way for unified and unambiguous recognition. The way to achieve this is by creating a common European-wide certification scheme (framework) that will ensure the basic requirements are fulfilled and that could be used as a basis for the accreditation of organizations providing Cybersecurity Skills Certifications.

This document aims to provide such a framework (a series of principles) that should be adhered to when creating a Cybersecurity Skills Certification Scheme, in order to achieve the above mentioned goals.

2. (Generic) Principles of Certification of Persons

2.1 Related Terms and Definitions

Jobs, roles and competences are terms commonly used when describing the actions, responsibilities, tasks and skills of people in the workplace. The terminology is often used interchangeably but still, before proceeding further, it is important to provide definitions of relevant and frequently used.

Term	Definition	Reference
Competence	Demonstrated ability to apply knowledge, skills and attitudes to achieve observable results. Competences form part of the Role Profiles. A demonstrated ability to apply knowledge, skills and attitudes for achieving observable results.	(CEN, 2018[5]) (CEN/TC 428, 2020[6])
Job description	A detailed description of what a person does so that the particular job holder can have no doubt of their tasks, duties and responsibilities and who they report to. It contains precise information about competences, skills and knowledge required as well as practical information about health and safety and remuneration. Note: Job Descriptions are not included in the Role Profiles but they can be developed from the Profiles.	(CEN, 2018)
Knowledge	Body of facts, principles, theories and practices that is related to a field of work or study. An employee	(CEN, 2018) (NIST, 2018[7])

[4] https://ecs-org.eu/documents/publications/60101ad752a50.pdf

[5] CWA 16458-3:2018, European ICT professional role profiles - Part 3: Methodology documentation. Retrieved from Ecompetencies:https://www.ecompetences.eu/ict-professional-profiles/

[6] CEN/TC 428. (2020). Methodology of the e-cf.

[7] NIST. (2018). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Term	Definition	Reference
	needs to know the relevant selection of these to successfully perform in their job. Knowledge is a body of information applied directly to the performance of a function. Represents the "set of know-what" (e.g. programming languages, design tools…) and can be described by operational descriptions.	(CEN/TC 428, 2020)
Role	A role derives from an organisational need to get something done. It is an organisational requirement that can be met by assigning employees to carry out all or part of the tasks required to ensure that role is carried out. One person or team may have multiple roles.	(CEN, 2018)
Role Profile	An outline or general document which demonstrates clearly the relationship between specific activities/tasks in a role and the individual skills, competences and knowledge required to undertake them.	(CEN, 2018)
Skill	The ability to use know-how and expertise to complete tasks and solve problems. Skill is often defined as an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cybersecurity rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual. The ability to carry out managerial or technical tasks	(CEN, 2018) (NIST, 2018) (CEN/TC 428, 2020)
Work Roles	Work roles are the most detailed groupings of cybersecurity and related work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role.	(NIST, 2018)
Ability	Is competence to perform an observable behavior or a behavior that results in an observable product.	(NIST, 2018)
Task	Is a specific defined piece of work that, combined with other identified Tasks, composes the work in a specific specialty area or work role.	(NIST, 2018)
Attitude	The "cognitive and relational capacity" (e.g. analysis capacity, synthesis capacity, flexibility, pragmatism…). If skills are the components, attitudes are the glue, which keeps them together.	(CEN/TC 428, 2020)

2.2 Relevant Standards

Certification for persons is a way of providing assurance that the certified person meets the requirements of a specific certification scheme. Confidence in the respective certification schemes for persons is achieved by means of a globally accepted process of assessment and periodic re-assessments of the competence of certified persons.

The principles governing these processes mentioned above are included in the ISO 17024:2012 Standard[8].

The international Standard ISO/IEC 17024:2012 "Conformity assessment– General requirements for bodies operating certification of persons", provides a global benchmark for quality certification. During recent years, this standard, developed by the International Organization for Standardization (ISO), which represents members from 162 countries has changed the way certifications are offered and has harmonized expectations for what constitutes quality certifications throughout the world. This standard was developed by ISO based on the need for public protection by establishing that individuals have the required competencies to perform their job[9]. Organizations worldwide have recognized the standard as a critical requirement for personnel certification bodies that offer certification in many industries including diverse and critical areas related to public health, environment, and national security.

2.3 Certification Principles

The text below describes the basic principles that any Certification Scheme for Skills should adhere to in order to assure a higher level of consistency and quality of operation. It should be noted that any organization that wants to become an accredited certification body of persons, should apply the entirety of the ISO 17024 standard. The text below is an attempt to provide an overview of the basic principles for certification of persons, so that this may later (section 3) be adapted to the Cybersecurity domain.

2.3.1. Impartiality

ISO 17024 defines Impartiality[10] as the presence of objectivity. Where objectivity means that those conflicts of interest do not exist, or are resolved, so as not to adversely influence subsequent activities of the body providing the certification.

Note: Other terms that are useful in conveying the element of impartiality are: independence, freedom from conflict of interests, freedom from bias, lack of prejudice, neutrality, fairness, open-mindedness, even-handedness, detachment, balance.

For the legal entity[11] [hereafter certifying organization or certification body] that designs,

[8] INTERNATIONAL STANDARD ISO/IEC 17024, Second edition, 2012-07-01, Conformity assessment — General requirements for bodies operating certification of persons, ISO (International Organization for Standardization)

[9] Guidelines on Conformity Assessment – ISO / IEC 17024:2012, The European Union's 10th EDF Programme for Nigeria, United Nations Industrial Development Organization, Federal Government of Nigeria

[10] Definition 3.15 as well as notes 1 & 2, INTERNATIONAL STANDARD ISO/IEC 17024, Second edition, 2012-07-01

[11] § 4.1. Legal matters, INTERNATIONAL STANDARD ISO/IEC 17024, Second edition, 2012-07-01

creates and implements the certification scheme following this framework, this would mean that:

- The certifying organization shall act impartially in relation to its applicants, candidates and certified persons. [4.3.2]
- Policies and procedures for certification of persons shall be fair among all applicants, candidates and certified persons. [4.3.3]
- Certification shall not be restricted on the grounds of undue financial or other limiting conditions, such as membership of an association or group. The certification body shall not use procedures to unfairly impede or inhibit access by applicants and candidates. [4.3.4]
- The certification body shall be responsible for the impartiality of its certification activities and shall not allow commercial, financial or other pressures to compromise impartiality. [4.3.5]
- The certification body shall require its personnel to declare any potential conflict of interest in any candidate. [6.2.1]
- Certification of a person should be based on objective evidence obtained by the certification body through a fair, valid and reliable assessment, and not influenced by other interests or by other parties. [A.2.1 - GUIDELINES ON CONFORMITY ASSESSMENT – ISO/IEC 17024:2012]
- Completion of training may be a specified requirement of a certification scheme. The recognition/approval of training by the certification body shall not compromise impartiality or reduce the assessment and certification requirements. [5.2.1]
- Certification bodies shall prevent fraudulent examination practices. [7.4.3]

To support the impartiality of the certification process, the certifying organization shall put in place measures and procedures that would allow:

- The timely identification and resolution of conflicts of interest or threats to impartiality arising from every part of the certification process.
- The fair, equal and ethical treatment among all applicants, candidates and certified persons. This means that during the design of a certification scheme limiting conditions such as membership of an association or group or other undue financial or other limiting condition should not be included as pre-requisite. This does not include training which could be used as a specified requirement of a certification scheme. The recognition/approval of such a training by the certification body shall not compromise impartiality or reduce the assessment and certification requirements.
- The avoidance of compromise of impartiality due to commercial, financial or other pressures.
- The derivation of the outcome of the examination based on objective evidence through a fair, valid and reliable assessment, and not influenced by other interests or by other parties.

2.3.2. Responsiveness

The Cambridge Dictionary, Cambridge University Press 2022[12], defines responsiveness as the quality of having a reaction to something or someone, especially a quick or positive reaction.

For the legal entity [here after certifying organization or certification body] that designs, creates and implements the certification scheme following this framework, this would mean that:

- The effective resolution of complaints and appeals is an important means of protection for the certification body and interested parties against errors, omissions or unreasonable behaviour. [A.5]
- The certification body shall have a documented process to receive, evaluate and make decisions on complaints. [9.9.1]
- The certification body receiving the complaint shall be responsible for gathering and verifying all necessary information to validate the complaint. [9.9.6]
- Any substantiated complaint about a certified person shall also be referred by the certification body to the certified person in question at an appropriate time. [9.9.8]
- The complaints-handling process shall be subject to requirements for confidentiality, as it relates to the complainant and to the subject of the complaint. [9.9.9]
- The decision to be communicated to the complainant shall be made by, or reviewed and approved by, personnel not previously involved in the subject of the complaint. [9.9.10]
- The policies and procedures shall ensure that all appeals are dealt with in a constructive, impartial and timely manner. [9.8.2]
- A description of the appeals-handling process shall be publicly accessible without request. [9.8.3]
- The certification body shall be responsible for all decisions at all levels of the appeals-handling process. The certification body shall ensure that the decision-making personnel engaged in the appeals handling process are different from those who were involved in the decision being appealed. [9.8.4]
- Upon application, the certification body shall make available an overview of the certification process in accordance with the certification scheme. As a minimum, the overview shall include the requirements for certification and its scope, a description of the assessment process, the applicant's rights, the duties of a certified person and the fees. [9.1.1]

To enforce responsiveness within the certification process, the certifying organization shall put in place measures and procedures that would allow:

- To respond to the requests for information regarding the application and the certification process, to manage appeals and complaints regarding any part of the

[12] https://dictionary.cambridge.org/dictionary/english/responsiveness

certification process.

- The allocation of roles, responsibilities and authorities to specific individuals regarding the application, appeals and complaints handling processes.

2.3.3. Confidentiality

ISO 27000:2008[13] defines Confidentiality as the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

For the legal entity [hereafter certifying organization or certification body] that designs, creates and implements the certification scheme following this framework, this would mean that:

- Personnel acting on the certification body's behalf shall keep confidential all information obtained or created during the performance of the body's certification activities, except as required by law or where authorized by the applicant, candidate or certified person. [6.1.6]
- The certification body shall require its personnel to sign a document by which they commit themselves to comply with the rules defined by the certification body, including those relating to confidentiality, impartiality and conflict of interests. [6.1.7]
- The certification body shall have a legally enforceable agreement covering the arrangements, including confidentiality and conflict of interests, with each body that provides outsourced work related to the certification process. [6.3.1]
- The records (of applicants, candidates and certified persons) shall be identified, managed and disposed of in such a way as to ensure the integrity of the process and the confidentiality of the information. The records shall be kept for an appropriate period of time, for a minimum of one full certification cycle, or as required by recognition arrangements, contractual, legal or other obligations. [7.1.2]
- The certification body shall ensure that information obtained during the certification process, or from sources other than the applicant, candidate or certified person, is not disclosed to an unauthorized party without the written consent of the individual (applicant, candidate or certified person), except where the law requires such information to be disclosed. [7.3.3]
- The complaints-handling process shall be subject to requirements for confidentiality, as it relates to the complainant and to the subject of the complaint. [9.9.9]

To ensure confidentiality of information is retained within the certification process, the certifying organization shall put in place measures and procedures that would allow:

- The identification of the information processed by the certifying organization in relation to the certification process, the applicants, the candidates, the certified

[13] INTERNATIONAL STANDARD ISO/IEC 27000, Fifth edition 2018-02, Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO (International Organization for Standardization)

persons and the persons no longer having an active certification. (This includes information regarding the scheme itself such as guidelines, procedures, applications, exam materials, databanks etc.).

- The protection of the above-mentioned information to the degree necessary based on the sensitivity and the type of information. The protection measures implemented should be compatible to the relevant applicable regulations and legislation (including the ones relating to the processing of personal data).
- The implementation of appropriate agreements with personnel and other interested parties involved in the certification process covering amongst others issues of confidentiality, impartiality and conflict of interests.

2.3.4. Responsibility

The Cambridge Dictionary, Cambridge University Press 2022[14], defines responsibility as something that it is your job or duty to deal with.

For the legal entity [hereafter certifying organization or certification body] that designs, creates and implements the certification scheme following this framework, this would mean that:

- The certification body shall be responsible for, shall retain authority for, and shall not delegate, its decisions relating to certification, including the granting, maintaining, recertifying, expanding and reducing the scope of the certification, and suspending or withdrawing the certification. [4.2]
- The certification body shall have the financial resources necessary for the operation of a certification process and have adequate arrangements (e.g. insurance or reserves) to cover associated liabilities. [4.4]
- When a certification body outsources work related to certification, the certification body shall take full responsibility for all outsourced work. [6.3.2]
- The certification body has a responsibility to ensure that only those persons who demonstrate competence are awarded certification. [A.1.3]
- The certification body has the responsibility to obtain sufficient objective evidence upon which to base a certification decision. [A.6]
- The certification body shall document its organizational structure, describing the duties, responsibilities and authorities of management, certification personnel and any committee. [5.1.2]

To support the responsibility of the certifying organization is achieved and maintained within the certification process, the certifying organization shall put in place measures and procedures that would allow:

- The identification of the roles, responsibilities and authorities that are needed for the

[14] https://dictionary.cambridge.org/dictionary/english/responsibility?q=Responsibility

correct, effective and impartial operation of the certification process from beginning to end.

- The traceability of every decision in relation to the certification process and especially the issuance / revocation / re-issuance of a certificate, is maintained and supported by relevant objective evidence.
- The control of all processes relating to certification even if they are not carried out by own means and are entrusted to external (third) parties. The certifying organization shall be responsible for all processes, decisions and activities carried out under its control.
- The sustainability and correct operation of the certification activities through the provision of relevant, adequate and competent (when related to persons) resources.

2.3.5. Competence

ISO 17024 defines competence as the ability to apply knowledge and skills to achieve intended results.

For the legal entity [hereafter certifying organization or certification body] that designs, creates and implements the certification scheme following this framework, this would mean that:

- The certification body shall have sufficient personnel available with the necessary competence to perform certification functions relating to the type, range and volume of work performed. [6.1.2]
- The certification body shall define the competence requirements for personnel involved in the certification process. Personnel shall have competence for their specific tasks and responsibilities. [6.1.3]
- The certification body shall maintain up-to-date personnel records, including relevant information, e.g. qualifications, training, experience, professional affiliations, professional status, competence and known conflicts of interest. [6.1.5]
- When a certification body outsources work related to certification, the certification body shall ensure that the body conducting outsourced work is competent and complies with the applicable provisions of ISO 17024 [6.3.2]
- The certification body shall create certification schemes that will contain amongst others the required competence (also in terms of pre-requisites if applicable). [8.2]
- The certification body shall ensure the identification and alignment of the assessment mechanisms with the competence requirements. [8.4]
- The assessment shall be planned and structured in a manner which ensures that the scheme requirements are objectively and systematically verified with documented evidence to confirm the competence of the candidate. [9.2.3]
- Examinations shall be designed to assess competence based on, and consistent with, the scheme, by written, oral, practical, observational or other reliable and objective means. The design of examination requirements shall ensure the comparability of results of each single examination, both in content and difficulty, including the

validity of fail/pass decisions. [9.3.1]

- The certification body shall ensure during the recertification process that it confirms continued competence of the certified person and ongoing compliance with current scheme requirements by the certified person. [9.6.2]
- The selected recertification activity/activities shall be adequate to ensure that there is impartial assessment to confirm the continuing competence of the certified person. [9.6.4]
- The overall purpose of certification of persons is to recognize an individual's competence to perform a task or job. [A.1.2]
- The certification body has a responsibility to ensure that only those persons who demonstrate competence are awarded certification. [A.1.3]
- Certification of persons provides value through public confidence and trust. Public confidence relies on a valid assessment of competence, by a third party, reconfirmed at defined intervals. [A.1.4]

To support the demonstration of competence throughout all the activities of the certification process, as well as within each certification scheme, the certifying organization shall put in place measures and procedures that would allow:
(In terms of internal operations of the organization)

- The identification of the competencies that the various identified roles of the organization in relation to the certification process (from start to end as mentioned before) need in order to be effectively implemented.
- The identification of any deficiencies in relation to these competencies and the implementation of suitable corrective actions. (e.g. provision of further training etc).
- The selection of appropriate parties (internal and external) that possess the necessary competence in order to award them the appropriate roles, responsibilities and authorities.
- The verification in a timely manner of the possession of the necessary competence and the provision of further education and training to keep it current (as applicable).

(In terms of the certification schemes)

- Each certification scheme shall be created for a specific job role, and will be supplemented with the relevant task descriptions.
- For the correct and effective implementation of these tasks, the certification scheme shall identify the necessary competences (meaning knowledge, skills and abilities (if applicable). These competences could be identified as pre-requisites and as core competence requirements of the certification scheme.
- For each certification scheme suitable examination mechanisms shall be designed. These mechanisms shall be adequate to assess the competence described within the certification scheme in a systematic, consistent and impartial manner.
- The same principles that apply to the certification mechanism of the initial certification shall apply for the re-certification.

3. Principles of Certification of Persons adjusted to the Cybersecurity domain

3.1. Introduction

The following principles have been derived taking into consideration:

- publications in relation to the assessment of information and cybersecurity skills,
- the experience of the project team and
- the feedback from the piloting of the 1st Certification Scheme for skills – C3 by CONCORDIA (Certified Cybersecurity Consultant).

3.2. Impartiality

Regarding impartiality, the requirements described in ISO 17024 should be applied and the rationale explained in Section 2.3.1. of this document should be followed along with the following Cybersecurity domain requirements:

3.2.1. The certifying organization shall provide the necessary exam mechanism and related resources that would allow for the correct, ethical and impartial implementation of the examination mechanisms.

3.2.2. This would include the notification of the names of the applicants and candidates to the various roles of the certification process. (E.g. The names of the applicants, when receiving an application for certification should be provided to the required roles. If any of the people assigned such roles identify a threat to impartiality or conflict of interest, corrective actions should be implemented. The same applies for the rest of the roles including examiners, invigilators etc).

3.2.3. The exam information from all examination platforms should be collected by the certifying organization in a way that guarantees their confidentiality and integrity.

3.2.4. The above requirement should be applied also in the case where some or all of the examination mechanisms are operated by third parties.

3.2.5. The examination mechanism (for theoretical and practical parts) should be suitable, allow for the collection of objective evidence, reliable and repeatable. There should be no option or mechanism to influence the results of the examination by any organizational role.

3.2.6. The only exception to the above should be the ability to provide a manual score in case that there is an error within the automatic grading process (if applicable) and in the case where the quality review performed / feedback received afterwards reveal an error to the examination material.

3.2.7. For the implementation of the theoretical exams, the certifying organization shall ensure that the question bank is checked and (if needed) updated on a periodic basis to ensure it reflects the evolution of the market.

3.2.8. For the implementation of practical exams through cyber ranges, the certifying organization shall retain a baseline of the relevant scenarios used in each examination and a relevant verification check will be implemented after each exam. (That the correct scenario was used and that the configurations do not deviate from the recorded baseline).

3.3. Responsiveness

Regarding responsiveness, the requirements described in ISO 17024 should be applied and the rationale explained in Section 2.3.2. of this document should be followed along with the following Cybersecurity domain requirements:

3.3.1. The certifying organization should provide information regarding the Cybersecurity Certifications in an open manner online. The information provided should at least provide the name and description of the Certification Scheme, the job and task description, the owner of the certification scheme, the pre-requisites, the language of the exam and a description of the examination mechanisms.

3.3.2. The above information should be provided at least in English if it is a Certification scheme that has a possible European wide range or at least in the local language of the Certification scheme owner if the scheme is a local – country wide one.

3.3.3. Especially for certification processes that are carried out in their entirety online, online contact information and methods should be implemented to facilitate communication to the scheme owner by the applicants, candidates and certified persons. The contact details should also include the working hours, the method that the contact team may reach back and an estimation of the response time (in average).

3.3.4. The website of the certifying organization and especially the area where information regarding contact details and methods, should include a suitable privacy policy and the visitor (site) should be informed regarding the processing of her/his personal data if they select to use the contact methods.

3.3.5. The information regarding the request of a person towards the certifying organization shall be collected, processed as needed, disclosed only to the roles needed (policies regarding least privilege and need to have should be applied) and retained as needed based on a specific retention policy. The retention policy shall be designed taking into consideration amongst others the purposes of processing and the current applicable legal and regulatory requirements.

3.4. Confidentiality

Regarding confidentiality, the requirements described in ISO 17024 should be applied and the rationale explained in Section 2.3.3. of this document should be followed along with the following Cybersecurity domain requirements:

3.4.1. The certifying organization shall identify all the information created and processed directly or indirectly in relation to the certification process. This includes information related to the publicly available information on the certification scheme, examinations and certificate register, the company confidential information of the examination materials, methods, configurations etc, the company related confidential personal information of the people involved in the certification process, the confidential personal information of the applicants, candidates and certificate holders etc.

3.4.2. For all the identified information (personal or non-personal) the certifying organization shall implement adequate security controls to ensure the confidentiality, integrity and availability of the information.

3.4.3. When third parties are involved in the certification processes, their operation will be governed by a suitable agreement which will include Confidentiality, IPR, availability and data transfers provisions according to the certifying organization's policies and in accordance to the applicable legal and regulatory requirements. Within this agreement, the role of the third party as a personal data processor will be clearly identified and the requirements as defined in Article 28 of GDPR and any other requirements required by local legislation shall be adhered to. The information shall be processed (by the processors) only on the documented instructions of the certifying organization which will include amongst others

a. Measures for ensuring that all information transmitted between all involved parties (processor, certifying organization, candidate, certificate holder, verifier etc) is in encrypted form with an acceptable level of encryption[15].
b. (If applicable) Measures for ensuring the security of the authentication process for applicants, candidates and certificate holders. (This would include passwords, multi-factor authentication, forgot password functions, captcha etc).
c. (If applicable) Measures for ensuring the robustness, availability and resilience of the platforms used.

3.4.4. All personnel, internal, sub-contracted and that of third parties, shall be bound by non-disclosure agreements for the duration of their engagement and for a period of 10 years after the termination of the engagement.

3.4.5. To ensure traceability and validation capability of certificates, the certifying organization shall retain a register of certificates that will contain at least the following information[16]:

[15] Acceptable levels of encryption may changed over time and the organization should may sure that the measures adopted provide adequate protection based on the criticality of the information. More information can be found at https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data)

[16] The retention period of the register should be defined within each certification scheme based on the relevant needs and the contractual, legal, regulatory and standards requirements.

- Certification Scheme
- Certificate Number
- Name, Surname of the Certificate Holder
- Date of certificate acquisition
- Date of certificate expiration
- The pre-requisites

3.4.6. The certifying organization shall provide the public an ability to verify the validity of a certificate at any point of time. This process shall be anonymous for the requester.

3.4.7. The validation and provision of information process shall be designed in a way that allows for the protection of the availability, confidentiality and integrity of the information. The process should be as automated as much as possible. (Where possible, blockchain implementation could be used).

3.4.8. Backups and any other measures deemed necessary shall be undertaken to ensure the availability, confidentiality and integrity of the information and the systems.

3.5. Responsibility

Regarding responsibility, the requirements described in ISO 17024 should be applied and the rationale explained in Section 2.3.4. of this document should be followed along with the following Cybersecurity domain requirements:

3.5.1. The certifying organization shall identify roles, responsibilities and authorities that are needed for the correct, effective and impartial operation of the certification process from beginning to end. These shall include at least:

a) Roles, responsibilities and authorities in relation to the creation of the databank for possible theoretical questions.

b) Roles, responsibilities and authorities in relation to the design and implementation of the scenarios for the possible practical exams through cyber ranges.

c) Roles, responsibilities and authorities in relation to the quality review of the databanks and the scenarios for the exams.

d) Roles, responsibilities and authorities in relation to the application process and the communication with the various interested parties (including the response and handling of appeals, complaints and any other requests).

3.5.2. The certifying organization shall have procedures in place for the response to information security incidents and personal data breaches. The procedures shall describe the processes, roles, authorities, responsibilities and activities that will be performed in such cases in line with the relevant applicable legislation and regulations.

3.5.3. The certifying organization shall have procedures in place with respect to checking and, when the case, updating the content of the theoretical and practical exams. The procedures shall describe the processes, roles, authorities, responsibilities and activities that will be performed in such cases, including the frequency of performing such operations.

3.5.4. The information that substantiates any decision of the certifying organization in relation to the certification process (from application to expiration / revocation of a certificate) shall be maintained by the organization. The organization if possible will include this information within an information system to ensure confidentiality, integrity, availability and non-repudiation.

3.5.5. The certifying organization shall monitor the systems used for the certification process, measure the availability and proceed in the correction of any identified issues.

3.6. Competence

Regarding competence, the requirements described in ISO 17024 should be applied and the rationale explained in Section 2.3.5. of this document should be followed along with the following Cybersecurity domain requirements:

(In terms of internal operations of the organization)

3.6.1. The certifying organization shall identify competencies for the various roles involved within the certification processes and especially for those mentioned in 3.5.1.

(In terms of the certification schemes)

3.6.2. The Cybersecurity skills certification schemes shall be based on identified role profiles defined within the European Cybersecurity skills framework. (Note: Since at the time of the drafting of this document the European Cybersecurity skills framework is still under development, other recognized international Role Profiles can be used, provided that in due time – and when the Role profile becomes available under the European Cybersecurity skills framework- procedures will be undertaken for its adoption.)

3.6.3. The adopted Role profiles shall contain at least the level of the Role, the knowledge, skills, tasks and (if applicable) the abilities that the professional bearing this role should have.

3.6.4. The level of the role should be compatible to the competence proficiency levels introduced in EN 16234-1:2019[17] as e-competence levels. These levels have already been related to the EQF[18] levels. E.g. Roles of e-CF level 1, have the ability to apply knowledge and skills to solve straight forward problems, is responsible for own actions and are operating in a stable environment.

3.6.5. The competencies identified within the Role Profiles used shall be compatible with CEN/TC 428, the 'e-Competence Framework' - EN 16234-1:2019, 2019

[17] https://www.en-standard.eu/bs-en-16234-1-2019-tc-tracked-changes-e-competence-framework-e-cf-a-common-european-framework-for-ict-professionals-in-all-sectors-framework/

[18] https://europa.eu/europass/el/description-eight-eqf-levels

and CEN Workshop agreement and 'European ICT Professional Role Profiles', CWA 16458-1, 2018. Especially for the soft skills needed (if they are not included within the above-mentioned documents), the relevant entries shall be compatible to those available in ESCO[19]. The competencies identified should cover also areas of applicable law, human factors/psychology, mathematics/cryptography, social sciences, economics, security & risk management/IT audit, etc[20].

3.6.6. For each identified knowledge and skill, the organization shall adopt a relationship between the e-competency proficiency level as applicable (e.g. If a given Role Profile contains → Dimension 1: A. Plan, Dimension 2, e-competency: A.6. Application Design, Dimension 3, e-competency proficiency levels 1,2 and 3, K2 Software development methods and their rationale, there would need to be a definition whether this knowledge (K2) is needed at a level 1, 2 or 3.) This will in turn allow for the definition of the content and level of the questions / tests that should be included in the examination for the validation of this knowledge. The same distinction should be applied for skills also.

3.6.7. In every examination, all knowledge and skills identified within the certification scheme shall be assessed.

3.6.8. Knowledge should be at least theoretically validated. The certifying organization may use multiple choice, open ended or scenario-based questions.

3.6.9. Since skills (see definition in section 2.1.) are more about applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual, the majority of the skills should be examined in a practical manner.

3.6.10. Roles identified in e-Competence levels 2-5 should test / verify the identified skills and knowledge (if desired) in a practical manner. The Certifying organization may decide to also test / verify the identified skills (if desired) in a practical manner also in the case of Roles identified in e-Competence levels (although not mandatory).

(Testing the Competencies)

3.6.11. For the theoretical examination of skills and knowledge the following should apply:

a) If possible, the theoretical examination platform should be integrated seamlessly with the platform used for the practical examination. If not possible, there should be a transparent and easy to use process and guide provided to the candidates prior to the commencement of each part of the exam. The security measures implemented within both platforms should be of the same high level and aligned with the requirements mentioned in 3.4.

[19] https://ec.europa.eu/esco

[20] ECSO Gaps in European Cyber Education and Professional Training https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf

b) The certifying organization should provide clear and appropriate information regarding the use of the platform and its abilities, at the latest when the candidate enters the theoretical examination environment for the first time. Time spent to reading these instructions should not count in the total examination time available. Prior knowledge of the specific platform should not be a pre-requisite for the successful implementation of the examination by the candidate.

c) The candidate shall have only one attempt, which would be timed. There should be a restriction on the time allocated for the theoretical exam.

d) Measures should be implemented to avoid the manipulation of the exam procedures and environment (including but not restricted to: Invigilators, secure browsing environment, cameras etc).

e) For every question posed within the theoretical exam, the certifying organization should retain a map of the reflecting the knowledge being assessed, the level of the knowledge, the complexity of the question, the grades awarded and the relevant conditions.

f) (If possible) The platform should be able to derive the score of this part of the exam automatically (if the questions are based on predefined answers or are multiple choice). In such cases the provisional score for this part of the exam should be provided to the candidate.

g) There should be a databank with a collection of questions that fulfil the requirements above and from which, a random / algorithm-based selection would be made for each examination. The certifying organization should make sure that enough questions exist to ensure that the same exam attempt is not repeated too often. The certifying organization should implement procedures for the regular update of the databank with up to date information.

h) A quality review process on the databank should be implemented at regular intervals or if complaints exist. If deficiencies are identified appropriate corrective actions should be implemented.

3.6.12. For the practical examination of skills and knowledge the following should apply:

a) If possible, the practical examination platform (cyber range or other simulation environment) should be integrated seamlessly with the platform used for the theoretical examination. If not possible, there should be a transparent and easy to use process and guide provided to the candidates prior to the commencement of each part of the exam. The security measures implemented within both platforms should be of the same high level and aligned with the requirements mentioned in 3.4.

b) The certifying organization should provide clear and appropriate information regarding the use of the platform and its abilities, at the latest when the candidate enters the practical examination environment for the first time.

Time spent to reading these instructions should not count in the total examination time available. Prior knowledge of the specific platform should not be a pre-requisite for the successful implementation of the examination by the candidate.

c) The practical exam (if practicable) should incorporate the verification of the relevant skills under one unified and comprehensive scenario. If possible, the questions / tasks requested to be performed by the candidate should not directly name the skill being tested but rather pose the question / task in the form of a specific goal. (E.g. The question should be "identify the devices that reside in your network and create the relevant network map" and not "Run the NMAP application, in order to find other assets within your network").

d) (If possible) The practical exam platform should be able to record the actions taken by the candidate within the environment and derive the existence of a skill by the actions implemented (or not implemented) and their sequence, even without reaching the overall goal.

e) For every scenario created the certifying organization should retain a map of the question / task / activity, the skills being assessed, the level of the skill, the grades awarded for each activity and the relevant conditions. If the system allows for hints, their use should be limited and with specific penalties imposed on grading if used by the candidate. A candidate shall not have the ability to use hints for every task to be performed.

f) (If possible) The platform should be able to derive the score of this part of the exam automatically. In such cases the provisional score for this part of the exam should be provided to the candidate.

g) There should be a collection of scenarios covering the same exam, fulfilling the above. The certifying organization should take care that enough scenarios exist to ensure adequate coverage based on the number of iterations per period. The certifying organization should implement procedures for the regular update of the scenarios with current information.

h) A quality review process on the scenarios collection should be implemented at regular intervals or if complaints exist. If deficiencies are identified appropriate corrective actions should be implemented.

i) Measures should be implemented to avoid the manipulation of the exam procedures and environment (including but not restricted to: Invigilators, secure browsing environment, cameras etc).

j) The candidate shall have only one attempt, which would be timed. There should be a restriction on the time allocated for the practical exam.

(Maintaining the competences)

3.6.13. The same principles that apply to the certification mechanism of the initial certification shall apply for the re-certification.

3.6.14. Special provisions shall be included in every certification scheme on the requirements that need to be fulfilled for the maintenance of the certification.

The cybersecurity domain is changing at a fast pace and it is crucial that a certified cybersecurity professional maintains his / hers knowledge and skills up to date during the period of validity of the certificate.

3.6.15. Each certification scheme shall explicitly define the period of validity of the produced certificates. Certification schemes should take into consideration the developments in the field when deciding on the period of validity of the certificates and the methods that they will ensure that the professional keeps his / hers knowledge and skills up to date.

For example, certificates with a one (1) year period of validity, are not expected to have additional requirements that would need to be fulfilled during this period by the cybersecurity professionals.

For certificates with a greater (thank one year) period of validity, the addition of further requirements is expected. Such additional requirements may be Continual Professional Education (CPE) credits / points. Such points could be earned by each cybersecurity professional through educational and implementation activities as appropriate.

It is recommended that practical skills and abilities are maintained through practical implementation activities and not solely through theoretical education and training.

3.6.16. In case that a certification scheme has such a CPE requirement, this should be clearly stated within the scheme documentation and a document containing CPE rules and instructions shall be created.

This document shall include amongst others: The definition of CPEs, the activities that are eligible to provide CPEs, the correspondence between the duration of these activities and the earned CPEs, the method of reporting CPEs and the method of CPEs validation.

The certifying organization shall have an interactive system that allows the cybersecurity professionals to view, submit, change, delete, report, access, object etc their CPEs per certificate.

3.6.17. The certifying organization shall have a platform or other system that allows for the management, access and maintenance of the information needed by the certificate holder. Suitable and adequate measures shall be enforced for the protection of the private information of the involved individuals. The platform or other system shall comply with the applicable privacy protection regulations and legislation. In every case, the rights of the data subjects shall be respected including the rights of rectification, erasure and restriction of processing.

3.6.18. Each certification scheme shall define the methods and conditions for the recertification of an individual. The period of re-certification shall be clearly identified. In case that the certification scheme, allows re-certification or certificate renewal, the details regarding how the lifecycle of the certificate will be depicted and available shall be explicitly defined.

4. Conclusions

This document provides information on the minimum requirements that should be implemented by a certifying organization when implementing certification schemes for cybersecurity skills.

These requirements can be seen as an expansion and specialization of a selection of the ones included in ISO/IEC 17024:2012 CONFORMITY ASSESSMENT — GENERAL REQUIREMENTS FOR BODIES OPERATING CERTIFICATION OF PERSONS, especially in the are of certification principles.

The document includes a number of requirements and information on the certification principles of Impartiality (8 requirements), Responsiveness (5 requirements), Confidentiality (8 requirements), Responsibility (5 requirements) and Competence (18 requirements).

The document could be used as a basis for next cybersecurity skills certification schemes in order to ensure a common baseline amongst related certifications.

Acronyms

DoA	Description of Action
CA	Consortium Agreement
EC	European Commission
EU	European Union
GA	Grant Agreement
WP	Work package
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission