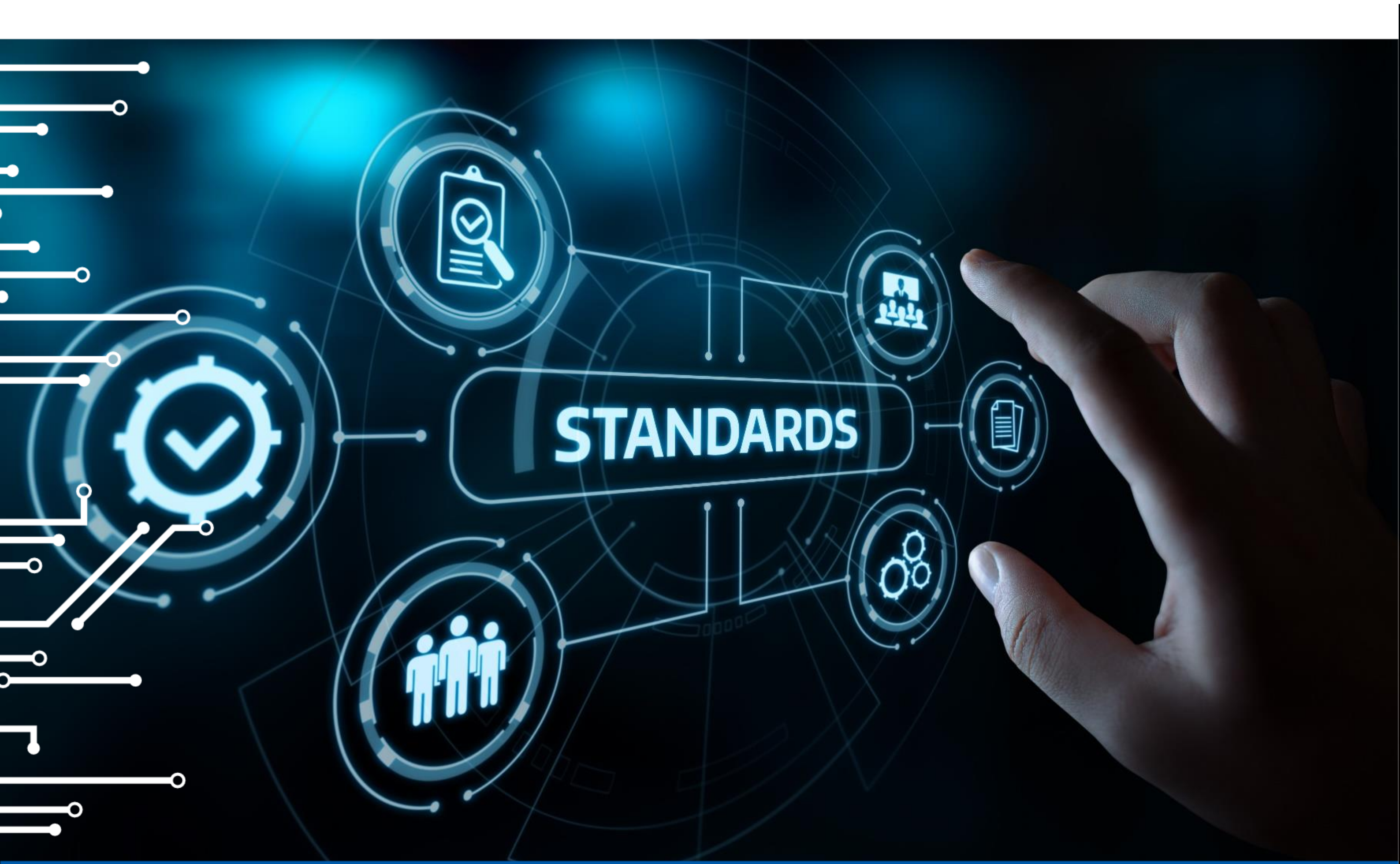
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



STANDARDISATION IN SUPPORT OF THE CYBERSECURITY CERTIFICATION

Recommendations for European standardisation in relation to the Cybersecurity Act

DECEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and servic es and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Sławomir Górniak – ENISA
Roland Atoui
Jesus Fernandez
Jean-Pierre Quemard
Martin Schaffer

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.
Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN 978-92-9204-328-5, DOI 10.2824/481787

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The EU Cybersecurity Act (CSA)[1] has made a dramatic change in the domain of cybersecurity evaluation by creating a single framework federating different evaluation schemes to harmonize Cybersecurity evaluation across the EU and therefore create a single European Cybersecurity Market.

The EU Cybersecurity Certification Framework makes it easier for ICT manufacturers and developers to serve the EU market. A unified certification framework across all of EU reduces the effects a fragmented market has on the economy. To support the creation of certification schemes under this framework the role of standardisation bodies is very important.

The SDOs (Standardisation Developing Organisations) will provide the necessary standards to support the framework to be defined by ENISA under request from the European Commission. There is a significant risk of creating inconsistent standards focused on vertical domains, despite the fact that cybersecurity is highly transversal. There is a strong necessity to create horizontal standards with a potential international coverage. The role of ENISA and its involvement in Standardisation tasks is essential, creating a harmonized frame to develop such standards.

Europe aims to be leading the cybersecurity certification and standardisation area for ICT products, processes and services. The EU Cybersecurity Act is an opportunity to have a harmonized market for cybersecurity. It brings a whole field of work, putting the consumers and the citizens in the centre of businesses' reflections and aims to improve EU cyber resilience and response by building upon existing instruments provided by SDOs keeping networks and information systems secure.

In this document, we present how valuable the cybersecurity standardisation efforts could be for certification, what are the roles and responsibilities of SDOs in this context, and how standardisation can support efficiently the process of certification schemes creation by following a step by step methodology.

The methodology described in this study could be used as guidelines for new certification scheme or standards authors. It will help setting up KPIs, useful for all stakeholders involved in the preparation or operational phase of a certification scheme. The qualification system proposed can be used also to define more precisely the requirements associated with the different assurance levels mentioned in article 52 of the Cybersecurity Act. “Assurance levels of European cybersecurity certification schemes”.

With regard to standardisation activities, we propose a set of recommendations for the Standards Developing Organisations and the prospective authors of certification schemes:

- The EU Union Rolling Work Program for standardisation should be aligned with the Union Working Programme for certification, in order for the SDOs to provide appropriate standards for the certification schemes
- Horizontal standards (multi sectorial) for cybersecurity must be privileged in cybersecurity evaluation but also in other domains as described in 3.1.
- It is very important to avoid competition between SDOs. In the EU ESO's cannot develop overlapping EN (European Norms). A coordinated joint approach between

[1] https://eur-lex.europa.eu/eli/reg/2019/881/oj

CEN, CENELEC and ETSI must be strongly encouraged and supported by the European Commission through adequate standardisation requests.

- When an international standard exists in a specific area and covers at least partially a targeted domain, it must be the preferred choice for usage.
- The competition and overlaps have to be carefully managed. The EU rolling plan can be an appropriate coordination tool to synchronize cybersecurity evaluation framework and associated standards.
- The ISO/IEC JTC1/SC27 should be considered as the first reference for cybersecurity standardization.
- It is important to improve the cooperation between CEN CENELEC JTC13 and ETSI TC Cyber and ensure that the majority of Cybersecurity standards and in particular in cybersecurity evaluation will be developed in joint working groups. This will guarantee that all relevant standardisation requests will be taken into account jointly.
- The ISO/IEC 15408/18045 Common criteria and evaluation methods, IEC 62443-4-2 Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components, EN 303-645 cybersecurity for consumer IOT can constitute the basis for all cybersecurity evaluation. They do not overlap, nor compete with each other, but can be seen as complementary. An introductory guide to the usage should be developed for the creators of certification schemes.

The Standard Developing Organisations (especially European ones – CEN, CENELEC and ETSI) have to interact in order to avoid overlapping contradictions or incompatibilities between standards and certification schemes. ENISA should participate in the relevant committees (CEN CENELEC JTC13 and ETSI TC CYBER as first priority), and encourage joint work between CEN CENELEC and ETSI, especially for topics related to the EU Cybersecurity Act implementation. To this aim, an interface mechanism between the Agency and the SDOs should be created, allowing for quick access to information concerning the standards in the certification areas under consideration.

1. INTRODUCTION

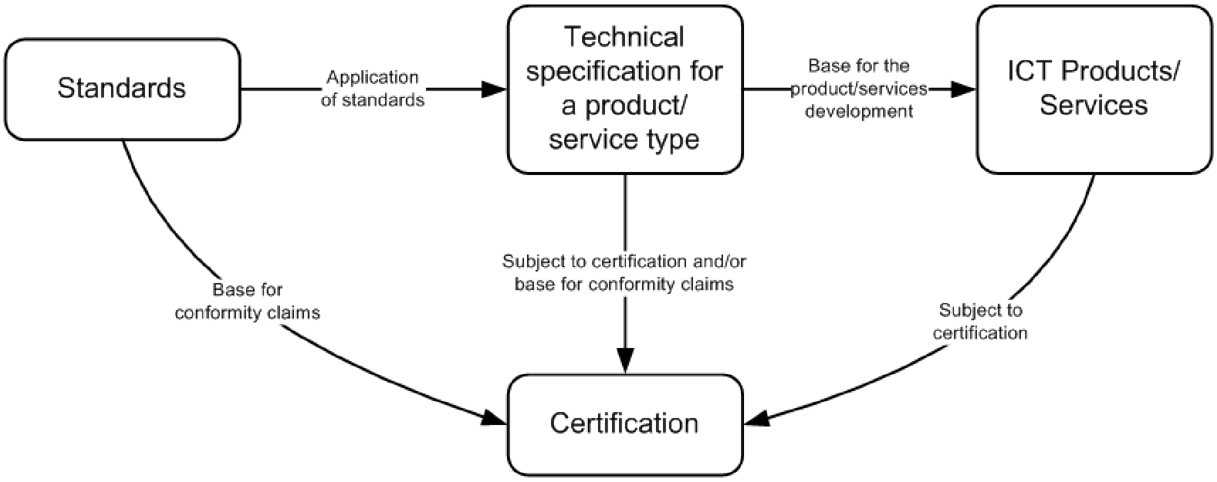
The EU Cybersecurity Act (CSA), which entered into force in June 2019, aims to establish a European cybersecurity certification framework for ICT products, services and processes. ENISA is participating in this new framework, by preparing candidate certification schemes on the request from the European Commission or the European Cybersecurity Coordination Group (representation of Member States).

Standardisation will play an important role in the framework, as the Act states the following:

- Recital 54: There is a need for closer international cooperation to improve cybersecurity standards, including the need for definitions of common norms of behaviour, the adoption of codes of conduct, the use of international standards, and information sharing, promoting swifter international collaboration in response to network and information security issues and promoting a common global approach to such issues.
- Recital 69: The European cybersecurity certification schemes should be non-discriminatory and based on international or European, unless those standards are ineffective or inappropriate to fulfil the Union’s legitimate objectives in that regard.
- Art. 52.4: The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto
- Art. 52.6: A European cybersecurity certification scheme shall include at least the following elements:
    - [..] references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements

A general concept for the role of standards in the evaluation and certification process is presented in the figure below.

Figure 1: Role of standards in the evaluation and certification process

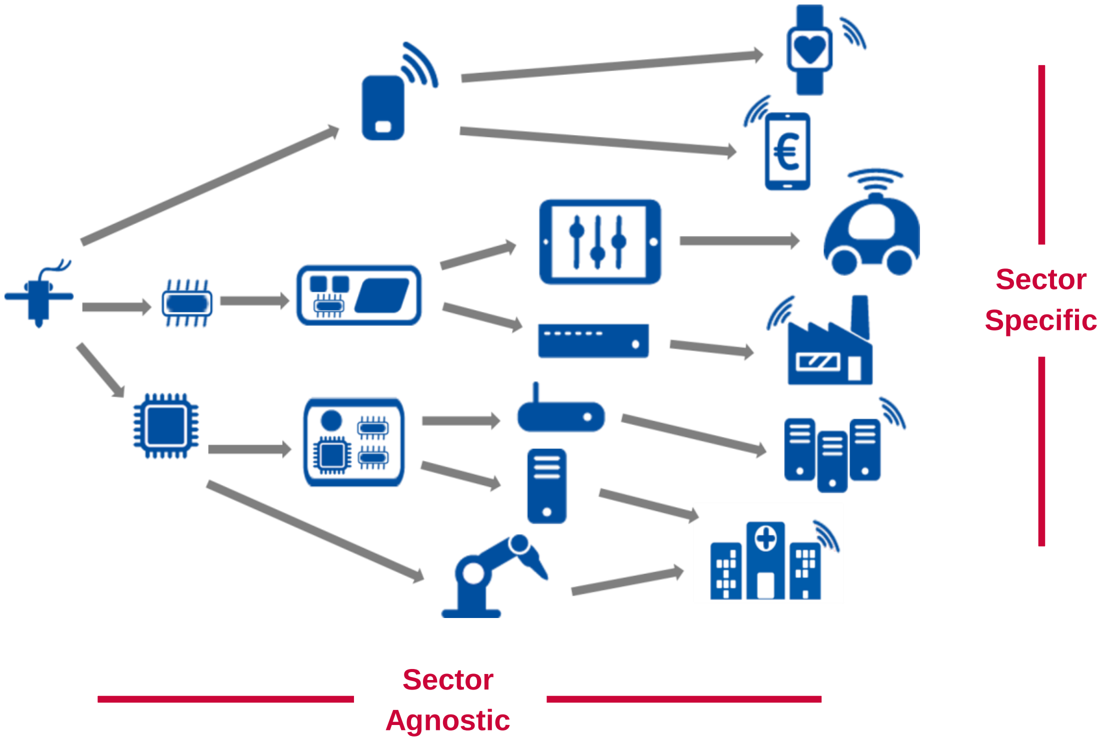

Standards
Application of standards
Technical specification for a product/ service type
Base for the product/services development
ICT Products/ Services
Base for conformity claims
Subject to certification and/or base for conformity claims
Subject to certification
Certification

Whenever a market needs to get regulated from cybersecurity perspective, it is essential to know:

- **what** a product, service or process shall fulfil in terms of cybersecurity requirements, and
- **how** to check that this is the case with the appropriate level of assurance (depending on the risk, the evaluation level targeted – basic, substantial, high – and impact of a potential attack).

However, this is not an easy task to implement. The challenge is that digital solutions are developed, produced, deployed, used and maintained in very complex eco-systems across the globe. Supply chains are very often not fully understood. Manufacturers of components, being rather at the start of the supply chain, often have no visibility in which final product their technology ends up (unless very specifically tailored for a use case). On the other hand, for OEMs it is quite difficult or even impossible to know where a dedicated component (a small chip embedded into the door of a car controlling the window) comes from. OEMs clearly know Tier 1 suppliers and maybe Tier 2. But further down the supply-chain the chance is very small to be able to make a proper tracing.

Figure 2: Example of supply chain for digital solutions



Accordingly, it is very important that standardization and certification approaches are well aligned across different industries when it comes to suppliers at the start of the supply-chain. For example, manufacturers of micro-controllers usually deliver their chips into multiple sectors. On the other hand, once the integration steps come close to a final product, the situation might become very sector-specific. Therefore, it is essential to keep at least two views in mind:

1. **The horizontal view**: standards for basic technologies, such as micro-controllers, whose final usage is not always clear, will most likely tend towards higher levels of cybersecurity in terms of robustness against a broad range of attacks. Accordingly, certification schemes used there need to be rather generic (e.g. ISO15408 – Common

Criteria) than specific and act as building blocks for certification schemes tailored to sectors.

2. **The vertical (sectorial) view:** standards in this case are typically very specific to the sectorial needs. However, to be efficient it makes sense to have those standards built on top of what the horizontal "catalogue" provides. This is also the case for certification schemes. Certification schemes very specific to sectors (e.g. IEC62443) should make use of horizontal (generic) schemes and recognize and build on top of those.

If these two views are not properly managed and considered, the industry will need extremely high efforts to comply with standards and participate in the certification processes. A manufacturer of a chip might need to run through many different certification schemes covering the same or similar requirements. Hence, the intention of this document is to bring clarity for any stakeholders impacted by the EU Cybersecurity Act when it comes to standardization in the sense of ***what*** to fulfil from cybersecurity perspective and in terms of ***how*** this can be checked accordingly with the appropriate level of cybersecurity assurance.

The remainder of this report is organized as follows: Section 22 summarizes the domains and benefits of standardization. Afterwards, section 3 explains the roles of standardization bodies followed by section 4, which provides a general description of what is a cybersecurity certification scheme and how the standards support certification. Section 5 proposes a structured methodology how the certification schemes can be drafted with support of standardization. Finally, section 6 draws final conclusions and recommendations, including the potential role of ENISA.

2. THE SCOPE AND VALUE OF CYBERSECURITY STANDARDISATION

2.1 THE DOMAINS OF STANDARDISATION

Standardisation activities take place in international, national, and industry-based fora. Within Europe, the three European Standards Organizations: CEN, CENELEC, and ETSI cooperate in order to minimize the duplication of standards. Many technical committees have liaisons and co-operation agreements within all the different technical standardisation committees. However, there are many hundreds of technical committees within the standards community that work on cybersecurity or have cybersecurity related work streams, and working in parallel. It has proved to be difficult to coordinate these activities, in particular due to the different scopes covered by the standardisation bodies and the lack of harmonisation between the terms and definitions used. Even the term cybersecurity[2] has different definitions and is often confused with IT security.

The scope of cybersecurity includes the protection of complex environments, resulting from the interaction of people, software and services on the Internet by means of technology – devices and networks connected to it. This is the consequence of the global digital transformation. All digital systems are concerned: IT of course, but also application domains, like healthcare, energy, automotive, cloud computing, IoT, etc.

For these reasons cybersecurity is highly transversal. Improving cybersecurity is necessary for all vertical domains.

The scope of cybersecurity is very broad and there are a high number of potential domains, which are candidates for standardisation:

- **Information security management processes** (ISMP): to define criteria, methods to guarantee the security of the management systems of a vendor, an operator, an end-user. These processes cover the entire lifecycle till the end of life and not only the development phase
- **Products, solutions and services design:** to check cybersecurity functions against risks and assess the functions and capabilities of products, solutions, services using technical means like Cryptography, public key infrastructures, secure by design principles, secure communications protocols,
- **Cybersecurity and certification** evaluation criteria, evaluation methods, hardware module evaluation, side channels attacks evaluation, random bit generators evaluation,
- **Evaluation laboratories evaluation**: people evaluation, development processes evaluation, malware testing, penetration testing, static code analysis and binary analysis.
- **Maintenance and operations of the cybersecurity**: security operation centre management, security operation centres indicators, vulnerability management, vulnerabilities format,

[2] Please see: Definition of Cybersecurity - Gaps and overlaps in standardisation, ENISA 2016, https://www.enisa.europa.eu/publications/definition-of-cybersecurity

- **Standardizing stakeholder security procurement and subcontracting processes:** contract and subcontract management, product decommissioning and product labelling, supply chain integrity and security, fraud and counterfeit management.

2.2 THE BENEFITS OF STANDARDISATION.

The benefits of standardisation in cybersecurity are clear and well known: Interoperability, reusability, knowledge development and cybersecurity awareness, harmonisation of terminology, consistency between different manufacturers, vendors and users, repeatability, performance checking, security evaluation, supply chain integrity and security.

In the particular case of cybersecurity evaluation, on the one hand standardisation is necessary: security risk evaluation, security target, protection profile, evaluation criteria, evaluation methods, maintenance of cybersecurity certificates along the life cycle. On the other hand, consistency between evaluations performed by different laboratories is a key issue. For example,tandards must be developed to support the evaluation of the evaluator, peer review management, etc. Standardisation is likely to warrant the necessary consistency of cybersecurity evaluation all over the EU and potentially worldwide, in order to create a harmonised cybersecurity worldwide market. The main objective being to guarantee that any evaluation of cybersecurity made in any of the EU member state is valuable and accepted for all EU Member States, and that there is no need to carry out multiple evaluations.

Another important point is that evaluation under the cybersecurity security certification framework will also introduce new requirements, for example, different assurance levels (basic, substantial and high) to cover different risk analysis. It is very important to be able to certify products, solutions and services at a level that is consistent with risks to be mitigated, but also taking into account the market needs (cost, time and performance to be achieved). The cost of evaluation cannot and must not be the same between nuclear, space or defence devices, and simple Internet-connected thermometers of an in-house weather forecast station; but instead it must be commensurate with the purpose the target of evaluation, serves. Impact of eventual cyberattacks will be considerably different in the given examples. It is very important to be able to fine-tune the cyber security evaluation according to the risk evaluation. This will need to be standardised as well, considering operational use and lifecycle management

For these reasons there is need to define and standardise cybersecurity evaluation criteria and evaluation methods.

Due to the transversal nature of cybersecurity, standardisation is a solution to avoid the creation of multiple cybersecurity evaluation frameworks according to different vertical sectors – automotive, healthcare, Cloud infrastructure, IoT, 5G, energy, etc. It is important to reuse standards to serve a multi-sectorial approach. Consistency across vertical sectors will assure minimum viable expectations for cybersecurity and will support greater uptake and adoption.

There are high risks associated with vertical domains developing their own set of cybersecurity evaluation of standards for many reasons:

- Ignorance of the existing standard base,
- Intended willingness to simplify what is perceived as too complex,
- Perceived specificity of the considered industrial domain,
- Low knowledge base of the stakeholders.

3. THE ROLE OF STANDARDISATION BODIES

3.1 ASPECTS OF STANDARDISATION BODIES

Standardisation bodies have different scopes and governance. The section hereinafter concisely presents them.

3.1.1 International level SDOs:

ISO, IEC, ITU, under UN governance are recognized by the standardisation community as international standard organisations (SDO). These organisations are potentially addressing all domains. The members of these SDOs are registered national bodies (NB). They are mostly working on a consensus basis, but voting is an exceptional case, in which the principle chosen is “one member one vote”. That is to say that each state has the same weight in a vote, whatever the size of the country. Generally, standards published are available for a fee.

3.1.2 The EU level

In the EU there are three recognized standardization bodies: CEN, CENELEC, and ETSI. These ESOs (European standardization organizations) are partly funded by the European Union.

CEN and CENELEC function in a similar manner to ISO and IEC, the membership is also assured through national bodies. They have an increasingly more integrated functioning through CCMC (CEN CENELEC Management Centre). The published standards are generally not free.

ETSI has a different governance organization from CEN and CENELEC. Membership is assured via individual registration from companies coming from all the Member States. The membership fee is paid on a voluntary basis and the number of votes is proportional to the annual fee cost. There are regulations and governance mechanisms in place, in order to avoid the majority shared by only a few members. There is also a national representation for the European matters (like European standards ballots).

One important point is that ETSI standards and all technical reports and technical specifications are available free of charge. This guarantees a high acceptance of standards worldwide.

3.1.3 Ad hoc standardisation bodies

In addition to the official international or European standardization bodies, there are other entities working in specific and focused domains, for example industrial fora like 3GPP, CSA, Fido Alliance, Global platform, IEEE, IETF, AIOTI, one M2M, TCG, Oasis etc.

These industrial bodies have different ways of functioning depending on their scope, participation and coverage, but they intend to cover specific requirements from industry and claim to be more efficient than traditional SDOs. Nevertheless, they do not have the official recognition that the international SDOs have. However, the international SDOs have defined specific procedures to import the de facto standards from these organisations, like PAS (publicly available specifications), or so-called fast track mechanisms. This approach proved to be very useful, as a good example we can note ISO 27000, which was created as BS 7799 and transposed to an ISO/IEC standard using a fast track procedure.

It can be noted that national standardisation bodies are also producing high value standards, like for example the US NIST – National Institute of Standards and Technology. One of the

NIST standards, the FIPS 140-2, has been taken as a basis to develop ISO/IEC 19790 – Cryptographic module evaluation. This ISO/IEC standard became afterwards the reference for the revision 3 of the FIPS 140.

3.1.4 Transposition of standards

In order to authorize exchange and transfer of standards between International and European SDO's, mechanisms of transposition have been put in place (Dresden, Frankfurt and Vienna agreements), authorizing to transpose standards from one standardisation body to another without restarting all work from scratch. It is possible, for example, to transpose an IS (International standard) to an EN (European standard) to be referred to in European regulations, or to transpose an EN in an IS in order to make it applicable worldwide.

The Vienna Agreement, signed in 1991, was drawn-up with the aim of preventing duplication of efforts and reducing time when preparing standards. As a result, new standards projects are jointly planned between CEN and ISO. Wherever appropriate, priority is given to the cooperation with ISO, provided that the international standards meet the EU legislative and market requirements, and that non-EU global players also implement these standards.

CENELEC enjoys close cooperation with its international counterpart, the International Electrotechnical Commission (IEC). In order to facilitate a consensus-finding process between European and international standards development activities in the electrical sector, CENELEC and IEC formalized the framework of their cooperation through the signature in 1996 of an “agreement on common planning of new work and parallel voting”, known as the Dresden Agreement.

After 20 years of a fruitful partnership, this has resulted in a very high level of technical alignment (close to 80% of CENELEC standards are identical to or based on IEC publications). CENELEC and IEC have reconfirmed their longstanding cooperation on 17 October 2016, by signing the Frankfurt Agreement. Building on the experience of both partners, this new agreement preserves the spirit and approach conveyed by the Dresden Agreement, in particular the strategic commitment of CENELEC to support the primacy of international standardization. It includes several updates aiming at simplifying the parallel voting processes and increasing the traceability of international standards adopted in Europe thanks to a new referencing system.

3.1.5 Overlaps in standards

Cybersecurity standardisation activities take place in international, national, and industry-based fora. Within the EU, the three European Standards Organizations, CEN, CENELEC, and ETSI cooperate to try to minimize the amount of duplication of standards. Many groups have liaisons and cooperation agreements within each other. Unfortunately, common understanding between these groups has proven to be difficult.

There are many examples of duplication of work between standards organizations. Without mentioning concrete examples, we can state that it can lead to at least duplication of efforts, and in the worst case in the inconsistent sets of standards, which is harmful for industry, as potential users of the standard. In addition, the relation of cybersecurity groups with other security domains (societal security, physical security etc.) is not sufficiently addressed.

We can note the recent creation (2019) within CEN and CENELEC of a cybersecurity sectorial forum in order to address this gap. This forum has identified 14 primarily relevant standardisation bodies for cybersecurity within CEN and CENELEC, for which improved collaboration is necessary:

- CEN/CLC/JTC 4 Services for fire safety and security systems
- CEN/CLC/JTC 8 Privacy management in products and services

- CEN/CLC/JTC 13 Cyber security and data protection
- CEN/TC 72 Fire detection and fire alarm systems
- CLC/TC 79 Alarm systems
- CEN/TC 79 Respiratory protective devices
- CEN/TC 162 Protective clothing including hand and arm protection and lifejackets
- CEN/TC 164 Water Supply
- CEN/TC 192 Fire and rescue service equipment
- CEN/TC 234 Gas Infrastructure
- CEN/TC 263 Secure storage of cash, valuables and data media
- CEN/TC 325 Crime prevention through building, facility and area design
- CEN/TC 391 Societal and citizen security
- CEN/TC 439 Private security services

One the first tasks identified by the forum was to align terminology between all these groups and identify existing overlapping standards.

3.2 STANDARDISATION BODIES INVOLVED IN CYBERSECURITY

There is a plethora of bodies involved in cybersecurity standardisation, here we name the most important:

- **ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy Protection.**
  - This standardisation committee develops International standards for information security, cybersecurity and privacy protection. They have produced over 150 standards, including generic methods, techniques and guidelines to address both, security and privacy aspects, such as:
    - Security requirements capture methodology;
    - Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services: ISO/IEC 270XX family;
    - Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information, ISO/IEC 18033, ISO/IEC 29192, ISO/IEC 10118, ISO/IEC 15946;
    - Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
    - Security aspects of identity management, biometrics and privacy like ISO/IEC 24761, ISO/IEC 24745, ISO/IEC 24760, ISO/IEC 29100/29101, ISO/IEC 27101;
    - Conformance assessment, accreditation and auditing requirements in the area of information security;
    - Security evaluation criteria and methodology ISO/IEC 15408/18045 known as Common Criteria, and also ISO/IEC 19790/24759 Security module evaluation.
- **CEN CENELEC JTC13 Cybersecurity and Data Protection**
  - This committee develops standards for data protection, information protection and security techniques with specific focus on cybersecurity covering all concurrent aspects of the evolving information society, including:
    - Organizational frameworks and methodologies, including IT management systems
    - Data protection and privacy guidelines
    - Processes and products evaluation schemes
    - ICT security and physical security technical guidelines

        - Smart technology, objects, distributed computing devices, data services
    - JTC13 recognizes the value of International standards and intends to reuse as much as possible existing standards. JTC13 will identify and possibly adopt standards already available or under development, which could support the EU Digital Single Market, EU legal acts and standardization requests. If required, these standards will be complemented by Technical Reports (TR) and Technical Specifications. Special attention will be paid to ISO/IEC JTC 1 standards and in particular SC27 (see above), but is not be limited to this group. Other SDOs and international bodies are also considered, such as ISO, IEC, ITU-T, IEEE, NIST or industrial fora.
    - For the identified standards, mentioned above, two options are considered:
        - Direct adoption as European Norms (EN), using Vienna or Frankfurt agreements;
        - Adoption as EN with additional/complementary requirements, for example in order to fulfil the EU legal requirements.
    - The list of already transposed standards is available at the committee's web page[3].
    - CEN CENELEC JTC13 is also organizing in coordination with ETSI TC Cyber dedicated events on cybersecurity standardisation, with the support of CCMC (CEN CENELEC management centre) and ENISA
- **ETSI TC CYBER**
    - the ETSI TC CYBER (Cybersecurity) intends to cover:
        - Cyber Security Standardization from a generic point of view
        - Security of infrastructures, devices, services and protocols
        - Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators
        - Security tools and techniques to ensure security
        - Creation of security specifications and alignment with work done in other Technical Committees and International Study Groups
    - It coordinates work with external groups such as the CEN/CENELEC JTC13, the NIS Platform and ENISA. It collaborates with other SDOs (ISO, ITU, NIST, ANSI etc.). The committee answers to policy requests on cybersecurity and ICT security in broad sense.
    - For security evaluation, ETSI has published the TR 103-645 – Cybersecurity for consumer IoT, which will become the basis for a future EN.
- **Other relevant committees of standardization bodies :**
    - ISO/IEC JTC 1/SC 41 Internet of Things and related technologies
    - ISO/IEC JTC1/SC 38 Cloud Computing and Distributed Platforms
    - ISO/IEC JTC 1/SC 42 Artificial intelligence
      ISO TC22/SC32/WG11 Automotive cybersecurity.
- **Industrial Forum of interest:**
    - 3GPP/GSMA, for 4G/5G concerns
    - CSA, Cloud security has a liaison with ISO/IEC JTC1/SC27WG4
    - Fido Alliance,
    - Eurosmart
    - Global platform, has a liaison with IOS/IEC JTC1/SC27/WG3
    - IEEE,
    - IETF,
    - AIOTI,
    - one M2M,
    - TCG, has a liaison with ETSI TC CYBER

[3] https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2307986&cs=1E7D8757573B5975ED287A29293A34D6B

- Oasis, has a liaison with ETSI TC CYBER

The standardisation action to introduce these industrial and de facto standards has to be done with SDOs through special procedures called PAS (publicly available specifications or fast track, in order to provide a common EU legal and technical frame work.

The main standards used currently for cybersecurity evaluation are:

- ISO/IEC 15408/18045 – Common criteria and evaluation methods. These standards are under important revision at ISO/IEC JTC1/SC27 level
- IEC 62443-4-2 – Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components
- EN 303-645 – Cybersecurity for consumer IoT, which is a standard originally developed by ETSI and now managed under a joint agreement by ETSI CEN CENELEC. This a good example of future collaboration.

These three sets of standards can constitute the basis for a broad range of cybersecurity evaluations. While they do not overlap with each other they are complementary with each other. This has been for example identified in the domain of Industrial automated control systems (IACS). Nevertheless, due to their complexity, identifying unique application domains of each of these standards is not an easy task. However, such work should be performed in order to facilitate the understanding and the reference in the development of upcoming cybersecurity evaluation framework and in order to avoid to reinvent the wheel and redevelop new standards.

4. CYBERSECURITY CERTIFICATION SCHEMES

A cybersecurity certification of ICT products, processes or services (hereinafter the “target”[4] of a cybersecurity certification Scheme) is the provision of assessment and attestation that fulfilment of specified security requirements has been demonstrated. It is carried out by Conformity Assessment Bodies (CABs) in coordination with the vendors and service providers, who are commonly requested to provide evidence in a transparent manner reflecting the level of security. The CAB (evaluator) is expected to review this evidence and conduct applicable conformity assessment activities (design review, source code review, security functional testing, penetration testing, etc.) and generates an evaluation report which will be reviewed by the CAB (certifier) before taking the decision to grant a certificate if the requirements are satisfied.

4.1 OBJECTIVES AND PURPOSE OF THE CERTIFICATION SCHEMES

European cybersecurity certification schemes[5] constitute an important element in the new EU Cybersecurity Certification Framework for ICT products, services and processes introduced by the Cybersecurity Act.

The purpose is to ensure that the ICT product, process or service certified under one of these new cybersecurity certification schemes, complies with specified requirements supported by standardization organizations and the industry. This should help ensure the protection of the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions or services offered by, or accessible via ICT products throughout their life cycle.

The certificate issued by an accredited Conformity Assessment Body (CAB) will attest that an ICT product, process or service has been certified in accordance with such a scheme and that it complies with the specified cybersecurity requirements. The resulting certificate will be recognised in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product.

4.2 CYBERSECURITY CERTIFICATION SCHEME OWNER

The main responsibility of the Certification Scheme Owner is to maintain and update the Certification Scheme accordingly. It should operate within an industrial consortium composed of relevant Certification Scheme users.

The Certification Scheme Owner should be responsible for the objectives, the content and the integrity of the scheme, and must be able to:

- Maintain the scheme and provide guidance when required.
- Set up a structure for the operation and management of the scheme.
- Document the content of the scheme.

[4] In Common Criteria, this is called a Target of Evaluation or a TOE.

[5] An adopted European Cybersecurity Certification Scheme is a systematic organisation covering Evaluation and Certification of ICT products, ICT services and ICT processes under the authority of ENISA to ensure that high standards of competence and impartiality are maintained, and that consistency is achieved during the whole certification process.

- Ensure that the scheme is developed by persons competent in both technical and conformity assessment aspects.
- Make arrangements to protect the confidentiality of information provided by the parties involved in the scheme.
- Evaluate and manage the risks/liabilities arising from its activities.

4.3 CORE COMPONENTS OF A CYBERSECURITY CERTIFICATION SCHEME

According to Article 54 of the EU Cybersecurity Act, a candidate for the EU cybersecurity certification schemes must contain a list of elements (see annexes). Among these elements, the following three areas are necessary to build the core components of a cybersecurity certification scheme:

- A Technical Specification of Security Requirements for the target
- A specification of approved evaluation methods for the auditor / evaluators in charge of assessing the targeted ICT product, process or service
- The specification of requirements for bodies certifying the targeted ICT products, processes or services

When applicable, these three core elements are defined by standardization bodies. Otherwise, they could be specifically defined during the creation of the cybersecurity certification scheme.

The content and purpose of each component are described below.

4.3.1 Technical Specification of Security Requirements for the ICT product, process or service

This document contains the collection of technical requirements describing the desired cybersecurity behaviour expected for the target covered by the certification scheme

4.3.2 Assessment Methodology

This document presents a set of validation procedures required to assess the target against the technical specification requirements identified previously. It defines “How” the evaluator should validate the target to prove the required level of security assurance. This mainly covers the following aspects:

- Definition of the concept of evaluation methodology (docs review, vulnerability assessment, test procedures, Automation, Robustness, etc.)
- Definition of the concept of composition methodology (if applicable)
- Definition of the expected evaluation results (report, label, etc.)

4.3.3 Specification of requirements for Conformity Assessment

This document describes the requirements on bodies certifying the target products, processes or services and defines all the policies and processes that govern the certification scheme.[6]

This will cover at least the following items:

- Planning and Preparation (scope definition, etc.)
- Application Procedure
- Evaluation Process
- Certificate Issuance

[6] For facilitation purposes this document can be based on the international standard ISO/IEC 17065:2012 Conformity assessment - Requirements for bodies certifying products, processes and services.

- Certificate Maintenance (life-cycle management, status, delta, upgrade, derivative, etc.)
- Vulnerability Disclosure, Patching & Assurance Maintenance
- Program Management (CABs accreditation policy, surveillance, conflict, roles and responsibilities, etc.)

5. STANDARDISATION IN SUPPORT OF CYBERSECURITY CERTIFICATION

As previously stated, there is a clear fundamental value for certification from cybersecurity standardization. It is necessary to set up a close relationship and a practical coordination with SDOs allowing a functional and efficient use of standards in support of certification. Coordination should be based on a clear procedure and a methodology allowing to communicate efficiently with SDOs and to study in a transparent and harmonised manner the public specifications while creating a new certification scheme.

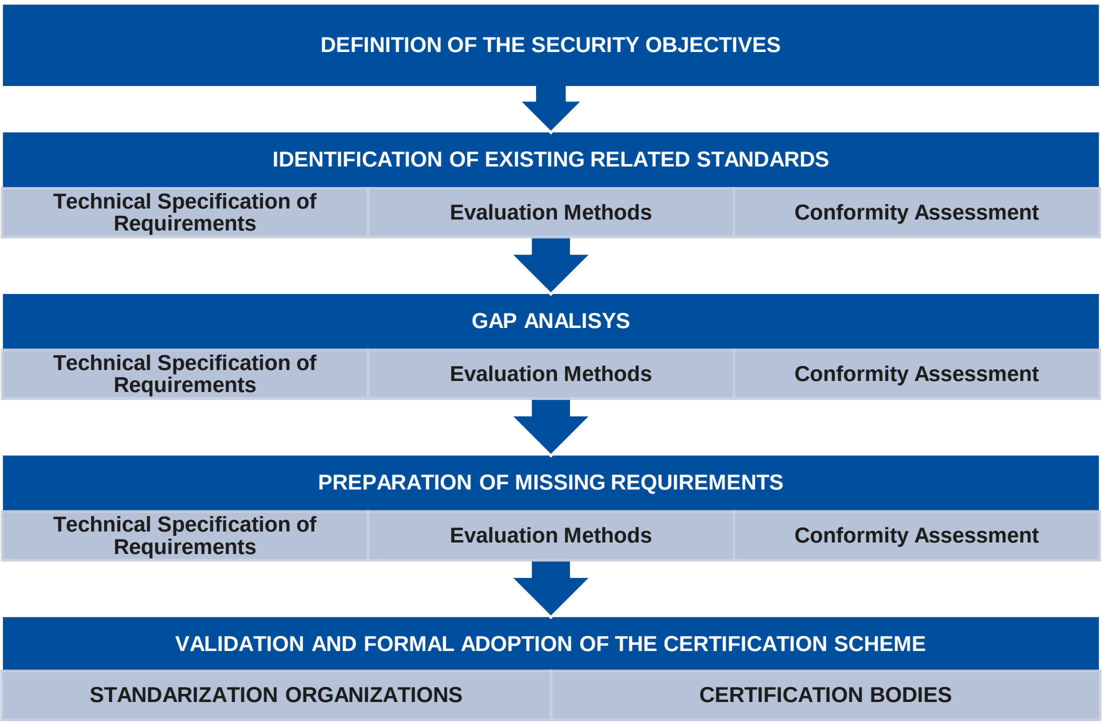
This section proposes an approach how to build a certification scheme, with fluent coordination with SDOs. More specifically, we define the steps to be followed, covering the definition of the security objectives and involving the industry stakeholders:

- the identification and classification of existing relevant standards
- a structured gap analysis methodology based on pre-defined qualification criteria
- the preparation of the final set of documentation filling the gaps
- the formal validation and adoption of the new certification scheme.

5.1 STEPS DEFINING A NEW CERTIFICATION SCHEME

The following diagram describe the drafting process and the different steps needed to develop a new certification scheme

Figure 3: Steps defining a new certification scheme



DEFINITION OF THE SECURITY OBJECTIVES

IDENTIFICATION OF EXISTING RELATED STANDARDS

Technical Specification of Requirements	Evaluation Methods	Conformity Assessment

GAP ANALISYS

Technical Specification of Requirements	Evaluation Methods	Conformity Assessment

PREPARATION OF MISSING REQUIREMENTS

Technical Specification of Requirements	Evaluation Methods	Conformity Assessment

VALIDATION AND FORMAL ADOPTION OF THE CERTIFICATION SCHEME

STANDARIZATION ORGANIZATIONS	CERTIFICATION BODIES

The procedures to develop in each stage is detailed in the following sections.

5.1.1 Stage 1. Definition of the security objectives

At this stage, the Certification Scheme Owner must identify the security objectives in coordination with the relevant industry stakeholders[7]. The security objectives are expected to be abstract statements, which in a formal way define the scope and the security properties that the target ICT product, ICT process or ICT service is intended to address.

The statements must concisely express the intended solution to the identified security problem. This could be a combination of assets, threats, policies and assumptions.

The method used to identify the security objectives could rely on existing standards defining a risk analysis approach such as ISO 27005, ISO 31000, EBIOS, MEHARI, e-IoT-SCS, Magerit, OCTAVE, etc.

5.1.2 Stage 2. Identification of the relevant standards in place

The Certification Scheme Owner must reach out to Standard Organizations to identify relevant standards covering the three main areas of the Certification Scheme:

5.1.2.1 Technical Specification of Requirements

The Standards Organization shall identify existing standards, specifying the technical requirements to meet the security objectives identified at Stage 1 for the target ICT product, process or service.

In addition, these requirements must cover “What” the vendor or service provider is supposed to provide as evidence proving a complete coverage of the security functional requirements.

- **Inputs: Security Objectives (Stage 1)**
- **Outputs: List of applicable Standard Technical Specification or Requirements**

5.1.2.2 Evaluation Methods

The Standards Organization shall identify existing standards specifying evaluation methods to assess the target against the technical specification of requirements identified previously.

- **Inputs: List of relevant Standard Technical Specification of Requirements**
- **Outputs: Inputs: List of applicable Standard Evaluation Methods**

5.1.2.3 Conformity Assessment

Standards Organizations and Notification Bodies shall identify existing standards providing guidance to Certification Bodies who wish to evaluate the conformity of target against the technical specification requirements identified previously.

- **Inputs: List of relevant Standard Technical Specification of Requirements**
- **Outputs: Inputs: List of applicable Conformity Assessment specification**

5.1.3 Stage 3. GAP Analysis.

[7] We strongly recommend at this stage involving regulatory organizations and all relevant authority implementing / using the certification scheme in a specific market to express the security risks acceptance and help in prioritizing the security objectives

During this stage, the Certification Scheme Owner is expected to qualify the selected applicable standards for each of the three areas and then identify missing areas to complete the coverage of all the contents described in the certification scheme.

5.1.3.1 Qualification of the existing standards

The measure of the quality in the cybersecurity evaluation and certification process is a paramount aspect to develop better and more efficient certification schemes that could at the end build trust by providing transparent and objective information to consumers and citizens about the level of cybersecurity of ICT products, services or processes

At the date of publication of the present report, a standardized system that could be used for qualifying the standards used in cybersecurity evaluation / certification does not exist. Due to the lack of this standard, this paper presents an initial proposal for a *Qualification System for Security Certification Schemes*.

Annex A describes the main components of a Qualification System and include an example with an initial proposal[8] for qualification criteria and a scoring system that can be used to qualify cybersecurity certification schemes

Classification system for the Certification schemes.

In addition to the parameters above and in order to qualify the certification scheme, the following includes a classification system for the certification schemes prepared with the aim to clarify and make easier the comparison process between them.

This classification system is not intended to qualify but rather to classify certification schemes in order to have a more objective comparison. It is expected to be used upfront of any qualification activity.

The Annex B includes a table with the proposed classification system for the cybersecurity certification schemes

5.1.3.2 Identification of missing requirements

This step is required to ensure that technical specification of requirements (identified at Stage 2) working together meet the objectives proposed for the Certification Scheme (mandated by the EU)

The Certification Scheme Owner is expected to run first a gap analysis on each of the three main parts of the scheme described above.

[8] Note: The qualification system defined in this paper, shall be understood just as an initial proposal for having a high level measure of the quality and the efficiency of the different certification schemes that will be developed in the framework of the Cybersecurity Act.

A further development of the qualification system shall be done improving the formalism and the alignment with the assurance structures of the actual standards used in cybersecurity evaluation and certification.

The authors of this study strongly recommend the international cooperation of Standardization Organizations and ENISA in the further development of guidance documents for the qualification system to ensure a general acceptance of the criteria and the procedures defined.

5.1.4 Stage 4. Preparation of the final set of documentation with missing requirements

- Request the SDOs and/or Certification Bodies to prepare a dedicated and complete specification of requirements for the Certification Scheme.
- Qualification of the final Certification Scheme in the terms of the Criteria used in stage 3 in order to make comparable certification Schemes

5.1.5 Stage 5. Validation and formal adoption of the Certification Scheme.

- Validation of the modified technical specification of requirements by the SDOs and the National Bodies (Formal adoption of the modified standards, with the new requirements… new standard or updating the old one)
- Formal adoption in ENISA of the final set of documents for the Certification Scheme.

6. CONCLUSIONS AND RECOMMENDATIONS

As the EU has been leading the cybersecurity certification and standardisation area for ICT products, processes and services, the EU Cybersecurity Act presents an opportunity to have a harmonized market for security. It brings a whole field of work, putting the consumers and the citizens in the centre of businesses' reflections and aims to improve EU cyber resilience and response by building upon existing instruments provided by SDOs keeping networks and information systems secure.

The EU Cybersecurity Certification Framework makes it easier for ICT manufacturers and developers to serve the EU market. A unified certification framework across all of EU reduces the effects a fragmented market has on the economy. To support the creation of certification schemes under this framework the role of SDOs is very important.

In this document, we presented how valuable the cybersecurity standardisation efforts could be for certification, what are the roles and responsibilities of SDOs in this context, and how standardisation can support efficiently the process of certification schemes creation by following a step by step methodology.

Building robust and sustainable certification schemes is not an easy task. It will require cooperation from a vast number of industries, SDOs and policymakers. However, the following recommendations can eventually reduce the risks of failure. Taking it one recommendation at a time is possible, as long as we understand what should come first: The higher accuracy defining the object of the cybersecurity certification (the target), the better option to define precise and detailed specification of security requirements (and by direct application higher assurance level for the certification scheme and higher trust levels for consumers)

The criteria listed for the qualification and classification system could be used as guidelines for new certification scheme or standards authors. It will help setting up KPIs useful for all stakeholders involved in the preparation or operational phase of a certification scheme.

The qualification system proposed can be used also to define more precisely the requirements associated to the different assurance levels mentioned in the article 52 of the Cybersecurity Act. “Assurance levels of European cybersecurity certification schemes”.

With regard to standardisation activities, we propose a set of recommendations for the Standards Developing Organisations and the prospective authors of certification schemes:

- The EU Union Rolling Work Program for standardisation should be aligned with the Union Working Programme for certification, in order for the SDOs to provide appropriate standards for the certification schemes
- Horizontal standards (multi sectorial) for cybersecurity must be privileged in cybersecurity evaluation but also in other domains as described in 3.1.
- It is very important to avoid competition between SDOs. In the EU ESO's cannot develop overlapping EN (European Norms). A coordinated joint approach between CEN, CENELEC and ETSI must be strongly encouraged and supported by the European Commission through adequate standardisation requests.

- When an international standard exists in a specific area and covers at least partially a targeted domain, it must be the preferred choice for usage.
- The competition and overlaps have to be carefully managed. The EU rolling plan can be an appropriate coordination tool to synchronize cybersecurity evaluation framework and associated standards.
- The ISO/IEC JTC1/SC27 should be considered as the first reference for cybersecurity standardization.
- It is important to improve the cooperation between CEN CENELEC JTC13 and ETSI TC Cyber and ensure that the majority of Cybersecurity standards and in particular in cybersecurity evaluation will be developed in joint working groups. This will guarantee that all relevant standardisation requests will be taken into account jointly.
- The ISO/IEC 15408/18045 Common criteria and evaluation methods, IEC 62443-4-2 Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components, EN 303-645 cybersecurity for consumer IOT can constitute the basis for all cybersecurity evaluation. They do not overlap, nor compete with each other, but can be seen as complementary. An introductory guide to the usage should be developed for the creators of certification schemes.

As stated above, the SDO's and mainly ESOs (CEN, CENELEC and ETSI) have to interact in order to avoid overlapping contradictions or incompatibilities between standards and certification schemes. ENISA should participate in the relevant work (CEN CENELEC JTC13 and ETSI TC CYBER as first priority), and encourage joint work between CEN CENELEC and ETSI, especially for topics related to the EU Cybersecurity Act implementation. To this aim, an interface mechanism between the Agency and the SDOs should be created, allowing for quick access to information concerning the standards in the certification areas under consideration.

A ANNEX: QUALIFICATION SYSTEM FOR CYBERSECURITY CERTIFICATION SCHEMES

Following is detailed an example of proposal of a qualification system for cybersecurity certification schemes.

The qualification system consist of two main parts:

1. The Identification of a suitable set of parameters for qualifying the quality of a certification scheme.
2. The definition of a scoring system for:
   a. Quantifying each parameter and expressing it numerically with the aim to make it measurable (and comparable).
   b. Pondering the different parameters according to their individual contribution level to meet the quality objectives of the certification scheme

Following sections describes in detail the different components of the qualification system proposed

1. QUALIFICATION CRITERIA (PARAMETERS AND SCORING RANK)

This section present an initial proposal of the criteria that can be used to qualify each one of the components of the certification schemes

1.1. Qualification Criteria for the Technical Specification of Requirements (TSR)

Definition process of the target of the certification

- Accuracy level determining the target of the certification

Accuracy level in the definition of the cybersecurity requirements is determined by the level of precision identifying the product where applicable.

The higher accuracy defining the target of the cybersecurity certification, the better option to define precise and detailed specification of cybersecurity requirements (and by direct application higher assurance level for the certification scheme and higher trust levels for consumers)

Scoring system: 1 (low) to 5 (high)

Table 1: Value Rank

Accuracy level	Level description
1	The precision level defining the object of the security evaluation is LOW. The target of the certification is a generic category of product, process or services
2	The precision level defining the object of the security evaluation is MEDIUM-LOW. The target of the certification is a generic category of product, process or services with a defined list of the component elements or the architecture of the system
3	The precision level defining the object of the security evaluation is MEDIUM. The target of the certification is a determined type of product, process or with a defined list of the component elements or the architecture of the system
4	The precision level defining the object of the security evaluation is MEDIUM-HIGH. The target of the certification is a specific product, process or services
5	The precision level defining the object of the security evaluation is HIGH. The object of the certification is a specific product, process or services with a precise definition of the internal components and the security behaviour

Other ponderation parameters:

- Use specific Security Profile/Protection Profile for each single type of products
  - Yes
  - No
- Operational Environment Consideration
  - Yes
  - Partially
  - No
- Composition certification allowed
  - Yes
  - No
- Other Schemes Evidence Re-use allowed
  - Yes
  - Partially
  - No

Definition process of the cybersecurity objectives for the target

There is not a single approach for the definition of the desired level of cybersecurity for a specific ICT product, service or process.

The definition process of the desired level of cybersecurity for a target is a risk assessment process weighting the potential threats and impacts for a determined intended usage of the target. (Different security levels can be defined for different conditions and environment of use of the target)

The desired security level is estimated by weighting the potential threats and impacts for a determined intended usage of the target. (Different security levels can be defined for different conditions and environment of use of the target)

- Accuracy level defining the cybersecurity objectives for target of the certification

Definition of the security objectives (expected security behaviour of the target) is the most relevant aspect to determine with precision what can be considered an appropriated level of security for the target.

The security objectives for a target can be expressed in terms of:

- A determined security behaviour of the target in a determined environment (expected use of the target)
- The resistance level of the target against specific attack methods

The higher accuracy defining the security objectives for the target, the better capacities to determine with precision and effectiveness the minimum cybersecurity requirements needed to achieve the desired cybersecurity behaviour of the target.

Scoring system: 1 (low) to 5 (high)

Table 2: Value Rank

Definition level of the security objectives	Level description
1	LOW. The security objectives are not specifically defined
2	MEDIUM-LOW. The security objectives are generally defined for the entire target
3	MEDIUM. The security objectives are generally defined for the entire target and different use conditions have been considered.
4	MEDIUM-HIGH. Security objective are defined at individual level for the target components Specific security objectives has been defined for specific use conditions
5	HIGH. A specific procedure is in place defining the security objectives for the target. Security objective are defined at individual level for the target components Specific security objectives are defined for individual security attributes (Confidentiality, Integrity, Availability) of the target components Specific security objectives has been defined for specific use conditions

Other potential ponderation parameters:

- A process is in place for defining the Security objectives of the target
  - Yes
  - No
- Security objectives consider the different security attributes (CIA) for individual components / information used in the target
  - Yes
  - No
- Different security objectives are defined for different cases of use of the target
  - No

    - Yes
    - Yes up to 3
    - Yes up to 5
- Security Objectives are properly defined through a risk assessment procedure
    - No
    - Yes
    - Yes, and the risk and the risk appetite clearly defined, expressing what is covered and what is not in the objectives
    - Yes, and the risk and the risk appetite clearly defined, for each intended usage scenario

Definition process of the evaluation areas covered in the assurance framework of the specification of requirements

A broader scope of evaluation areas offers higher assurance levels for the certification scheme and in the cybersecurity evaluation

Following are described main evaluation areas that can be considered for cybersecurity evaluation of targeted products, services and processes:

- <u>Documentation review</u>
    - Verifies if the vendor's implementation meets the requirements defined on design and guidance papers:
        - Guidance documents
        - Design plans
- <u>Audit of security procedures associated to the target</u>
    - Security in the design procedures,
    - Security procedures in the manufacturing process, and
    - Monitoring and maintenance cybersecurity procedures in the aftermarket process

  Ponderation parameters: Audit inspection level:
    - Documentation review
    - Onsite audit inspection of the vendors 'supply chain
- <u>Security functional testing</u>
    - Functional testing of cybersecurity functions implemented / used in the device
- <u>Robustness testing</u>
    - Stress test of cybersecurity functions and operational features implemented / used in the device
- <u>Vulnerability Analysis</u>
    - Check for public vulnerabilities in the product.
    - Potential ponderation parameters:
        - One time
        - Several times during the design and manufacturing process
        - Continuous monitoring system for new known vulnerabilities during the entire product life
- <u>Penetration Testing</u>
    - Tries to hack the target with the same methods and tools as real cyber-attackers .
    - Audit level can be modulated by the attack potential[9]. An attack potential is a numerically expressed attacker's potential that is required for executing attack scenarios for exploiting vulnerabilities in the target
    - For a methodical approach to produce comparable results a measure of target resistance against the different attacks methods covered in the

[9] The attack potential is formally defined in the international standard ISO 15408

penetration testing can be used. The use of international standards for evaluating the resistance of a target against specific attack methods will provide an added-value in terms of objectivity of the penetration testing procedures.

- Potential ponderation parameters:
    - Pentesting Style
        - Non
        - Not limited in Time
        - Time-Limited
        - Risk-Based + Time-Limited (per profile)
    - Measure the resistance of the product against different type of attacks procedures
        - Yes
        - Yes and based in international standards (For example ISO/IEC 17825)
        - No
        - Only some specific type of attacks methods (number of methods covered)
    - The attack potential is calculated for each attack method / or risk scenario used
        - Yes
        - No

Definition process of the technical specification of requirements included in each evaluation area

- <u>Criteria used in the definition / identification of security requirements included in each evaluation area.</u>
    - Criteria used identifying most appropriated set of security requirements needed to provide an appropriated level of security assurance for the target is one of the most relevant parameters that can be used to qualify a Certification Scheme.
    - Following are described main criteria that can be used for qualify the methodology of identification of cybersecurity requirement:
        - <u>Identification of high level Security Best Practices</u>
            - Identifying a list of high level cybersecurity controls or best guidance practices that could be commonly applicable to a generic category of products or services
        - <u>Identification of a list of Minimum Security Requirements</u>
            - Identifying a list of a specific cybersecurity requirements (minimum basic requirements) that could be applicable to specific type of products
            - Predefined list of cybersecurity controls that shall be implemented in the target
        - <u>Risk-based approach</u>
            - Conducting a risk assessment procedure to ensure that cybersecurity objectives determined for the expected use of the target are meet and the potential threats are properly mitigated by the cybersecurity requirements established
        - Ponderation parameters
            - A risk analysis is used in the drafting process of the cybersecurity requirements
            - Yes
            - Yes, and the Risk Analysis is based in a standardized risk assessment methodology

        - No
    - Scoring system: 1 (low) to 3 (high)

Table 3: Value Rank

Quality of the methodology for identification of security requirements	Level description
1	LOW. Security requirements are selected by Identifying a list of high level security controls or best guidance practices that could be commonly applicable to a generic category of products or services
2	MEDIUM. Security requirements are selected Identifying a list of a specific security requirements (minimum basic requirements) that could be applicable to specific type of products
3	HIGH. Security requirements are selected conducting a risk assessment procedure to ensure that security objectives determined for the expected use of the target are meet and the potential threats are properly mitigated by the security requirements established

1.2. Qualification Criteria for the Assessment Methodology

Definition process of the assessment methodology

Assessment methodology is one of the most relevant component in a certification scheme determining the level of objectivity in the evaluation process.

Assessment tasks include in some cases discretional procedures as including the expert opinion of a qualified evaluator in a specific question. These discretional processes are more often present in most advanced evaluations areas as vulnerability analysis or penetration testing.

- Criteria used for qualifying the objectivity level of the evaluation methodology:
    - The objectivity level of the evaluation methodology can be modulated trough different parameters or conditions which are applicable globally to the evaluation methodology itself or individually to specific evaluations procedures.
    - Following are described some parameters that can be used for qualifying the cybersecurity evaluation methodologies or the individual evaluation procedures:
        - Assessment Style
            - Third-Independent-Party Assessment
            - Self-Assessment with double review by different internal teams
            - Self-Assessment
        - Use evidence formalism (using a formal and structured language for specification of technical requirements and evaluation procedures)
            - Yes (CC, others)
            - Partially (CC + Natural Language)
            - No (Natural Language)
        - Produce comparable results
            - Yes

        - Partially
        - No
    - Objectivity level (associated to individual evaluation procedures)
        - 1 (low) to 3 (high)

Table 4: Value Rank

Objectivity level	Level description
1	The evaluation procedure is highly dependent on the discretional assessment of the evaluation team
2	The evaluation procedure is dependent on the discretional assessment of the evaluation team, but the procedure is modulated by the use of external qualifications requirements as technical knowledge of evaluators, years of experience, use of specific tools, etc.
3	The evaluation procedure is non-dependent on discretional assessments and always produce repeatable but not and comparable results

1.3. Qualification Criteria for the Conformity Assessment of the Certification Scheme

Conformity Assessment is one of the most relevant components in a certification scheme contributing to ensure the independency and the quality of the works done by the evaluator teams.

The rigorousness level in the specification of requirements for the conformity assessment will determine also the quality level of the certification process

Below are described some parameters that can be used for qualifying the conformity assessment procedures:

Market Surveillance

- Surveillance audits in certified products
    - Number of surveillance audits in certified products conducted by the CB, ensuring that the certified products and the manufacturer remain in compliance with the certification program and the published standard(s) under which the product is certified
    - Scoring System: 1 (low) to 3 (high)
    - Value Rank: Number of Surveillance Audits (SA)
        - SA< 2% of certified products: LOW
        - 2%<SA< 5% of certified products: MEDIUM
        - SA>5% of certified products: HIGH
- Public records of certificate metadata
    - A metadata certificate service allows to store (in a centralized or de-centralized way) properties related to the certified product such as the certification validity, scope, attestation, level of certification, etc.
    - These allows a service provider or a user to set up online cybersecurity policies allowing to authorize/accept a certified product.
    - Scoring System: Available YES / NO

Laboratories Surveillance

- Random Evaluations (RE)

  - Random evaluations with reference samples verifying the results obtained by the evaluation laboratory.
  - Scoring System: 1 (low) to 3 (high)
  - Value Rank: Percentage of accredited labs audited per year by the CB with a RE
    - Audited Labs < 2%: LOW
    - 2% < Audited Labs < 5%: MEDIUM
    - Audited Labs >5%: HIGH
- Round Robin Evaluations for inter-comparison (RRE)
  - Number of round robin tests conducted in different evaluations labs verifying comparable results are obtained
  - Scoring System: 1 (low) to 3 (high)
  - Value Rank: Percentage of accredited labs audited per year by the CB with a RRE
    - Audited Labs < 2%: LOW
    - 2% < Audited Labs < 5%: MEDIUM
    - Audited Labs >5%: HIGH
- Capacity level to maintain updated knowledge at the state of the art of the security (State-of –the-art Attack Methods and security requirements)
  - Procedures in the Certification Bodies ensuring an updated and shared knowledge between the evaluation labs of the state-of the-the-art Attack Methods and security countermeasures
  - Scoring System: 1 (low) to 3 (high)

Table 5: Value Rank

Procedures maintaining an state-of-the-art shared knowledge in security	Level description
1	Not specific procedures are in place in the Certification Bodies for maintain an updated knowledge at the state-of-the-art of the security. The technical specification of security requirements include all needed knowledge for conducting the evaluation. SDOs as owners of the TSRs, are in charge of maintaining the state of the art of the security requirement by periodical updates of the International Standards in the basis of the certification scheme
2	The state of the art in the security requirements for target of the certification is maintained by the Certification Body based in public sources of information, such as newspapers, public vulnerability databases, etc.
3	The Certification Body include in his organization specific working groups of technical experts structuring the state-of-the-art security evaluation knowledge for the evaluation laboratories and the Certification scheme

a) Verification process of the technical knowledge of Laboratories

Procedures in place in the Certification Bodies to verify the technical qualification of the Laboratories and the evaluators

Scoring System:

- 1 (low) to 3 (high)

Value Rank:

- LOW: Technical Qualification of the evaluation labs are granted by the general procedures of ISO 17025. Not specific procedures are in place by the certification body to verify the technical knowledge of the evaluation labs.
- MEDIUM: Evaluation Labs are in charge of the technical qualification of their evaluators and the evidence of the qualification is sent to the Certification Bodies
- HIGH Formal procedures are in place by the Certification Body for auditing the technical qualification of the laboratories and the evaluators. Technical qualification is periodically audited by the CB.

2. SCORING SYSTEM

2.1. Quantification system for the qualification criteria

A quantification system shall be defined expressing numerically the different values that the qualification criteria (parameters) can have.

Quantification system assign a value rank for each one of the different parameters used in this qualification system. (An example of the scoring rank proposed for each parameter is included in the previous section in order to facilitate the readability of the text)

2.2. Ponderation system and final score

A ponderation system shall be established defining the individual contribution level of each parameter addressing the quality objectives of the certification scheme.

Ponderation system is also used as calculation method of total score of the qualification system, as expressed in the next formula:

$$Total\ Score = \propto * \, P_1 + \beta P_2 + \cdots + \gamma P_n$$

Where α, β,γ, etc. are the ponderation rates and $P_{1\ldots}$ P_n the qualification parameters

The total score will measure the quality level associated to each certification scheme and indirectly can be used as a measure of the level of assurances and trust that would offer to consumers and citizens.

For simplification purposes, a simple table can be used for qualifying a certification scheme instead using the mathematical expression described above.

An example of a table describing a complete scoring system for a certification scheme is shown below:

Table 6: Example of scoring system

Component of the certification scheme	Nº	Qualification parameters	Quantification system Scoring rank	Assurance level value (over 500 points)
Technical specification of security requirements				
Object of the certification	1	Accuracy Level defining the Scope of the target	1 (Poor definition) to 5 (Highly detailed)	(25) 5 per level
	2	Use specific Security Profile/Protection Profile for each single type of products	YES /NO	(10) 10 / 0
	3	Operational Environment Consideration	YES / PARTIALLY / NO	(10) 10 / 5 / 0
	4	Composition certification allowed	YES /NO	(5) 5 / 0
	5	Other Schemes Evidence Re-use allowed	YES /NO	(5) 5 / 0
Security Objectives for the target	6	Definition Level of the Security Objectives	1 (Poor definition) to 5 (Highly detailed)	25 (5 per level)
	7	A process is in place for defining the Security objectives of the target	YES /NO	(10) 10 / 0
	8	Security objectives consider the different security attributes (CIA) for individual components / information used in the target	YES /NO	(10) 10 / 0
	9	Different security objectives are defined for different cases of use of the target	# NO # YES # YES up to 3 # Yes up to 5	(15) 0 / 5 / 10 / 15

	10	Security Objectives are properly defined through a risk assessment procedure	# NO # YES # YES and the risk appetite is clearly defined, expressing what is covered and what is not in the security objectives # YES and the risk appetite is clearly defined, for each intended usage scenario	(25) 0/10/15/ 25
Evaluation areas covered by the TSR	11	Documentation review	# NO # Yes. Guidance documents # Yes. Guidance Documents and Schematics and Design Plans	(10) 0 / 5 / 10
	12	Audit of security procedures associated to the target	# NO # YES. Security in the design procedures, # YES. Security procedures in the manufacturing process #YES. Monitoring and maintenance security procedures in the aftermarket process	(25) 0+5+10+ 10
	13		# Documentation review # Onsite audit inspection of the vendors ‘supply chain	(10) 0 / 10
	14	Security Functional testing	#NO # YES Partially Functional testing of some security functions implemented / used in the device # YES Functional testing of all security functions implemented / used in the device	(10) 0 / 5 / 10
	15	# Robustness testing	# NO # YES Stress test of security functions and operational features implemented / used in the device	(10) 0 / 10

	16	# Vulnerability Analysis	# NO # YES. One time # YES. Several times during the design and manufacturing process # YES. Continuous monitoring system for new known vulnerabilities during the entire product life	(15) 0/ 5 / 10 / 15
	17	# Penetration Testing	#. No # YES. Risk-Based + Time-Limited (per profile) # YES. Time-Limited #. YES. Not limited in Time	(25) 0/15/20/25
	18		# Include the measure the resistance of the product against different type of attacks procedures (NO/YES/Yes, based in standardized methods)	(15) 0 / 10 / 15
	19		# The attack potential is calculated for each attack method / or risk scenario used (NO/YES)	(15) 0 / 15
Methodology for identification of requirements	20	Quality of identification methods	# Best Guidance Practices # Predefined List of minimum security requirements # Risk based methodology # Standardized Risk based methodology	(25) 5/10 /15/ 25
EVALUATION METHODOLOGY				
Definition process of the evaluation methodology	21	Objectivity of the evaluation methodology	# Self-Assessment # Self-Assessment with double review by different internal teams # Third-Independent-Party Assessment	(35) 0 / 15 / 35
	22	Use evidence formalism	# No (Natural Language) # Yes, partially (CC + Natural Language) # Yes (CC, others)	(15) 0 / 5 / 15
	23	Produce comparable results	# No # Yes	(50) 0 / 50
CONFORMITY ASSESSMENT				

Market Surveillance	24	Surveillance audits in certified products	1 (Low level) to 3 (High Level)	(10) 0 / 5 / 10
Laboratories Surveillance	26	Random Evaluations	1 (Low level) to 3 (High Level)	(10) 0 / 5 / 10
	27	Round Robin Evaluations	1 (Low level) to 3 (High Level)	(25) 0 / 15 / 25
	28	Procedures Maintaining A State-Of-The-Art Shared Knowledge In Security	1 (Low level) to 3 (High Level)	(30) 0 / 15 / 30
	29	Audit of Technical knowledge	1 (Low level) to 3 (High Level)	(15) 0 / 10 / 15

TOTAL SCORE: 500 (MAXIMUM VALUE OF THE ASSURANCE LEVEL)

B ANNEX: CLASSIFICATION SYSTEM FOR CYBERSECURITY CERTIFICATION SCHEMES

Component of the certification scheme	Qualification parameters	Description
Target Market	Consumer	Scheme dedicated to ICT products, processes or services dedicated to the Consumer market. These must have NO safety risks due to cyberattacks but mostly where privacy risks come in priority.
	Enterprise	Scheme dedicated to ICT products, processes or services ending up in an enterprise IT environment. Financial risks, impacts on image and confidentiality of sensitive assets come in priority.
	Industrial	Scheme dedicated to ICT products, processes or services ending up in an industrial IT/OT environment. Financial risks and impacts on availability of the services come in priority.
	Critical	Scheme dedicated to ICT products, processes or services dedicated to the Consumer, Enterprise and Industrial markets. These must have safety risks due to cyberattacks compromising critical assets.
Target Users	Chip/HW Vendor	Scheme covering a target including the Hardware components. Hardware interfaces are used to evaluate the target. Targeted users of such scheme are typically ICT products manufacturers.
	ROE/RoT Developer	Scheme covering a target including the Restricted Operation Environment or Root of Trust software. Targeted users are OEMs or Platform suppliers.
	OS/FW Code Developer	Scheme covering a target including a rich Operating System or Firmware. Targeted users are mainly OEMs or Firmware developers
	Product Integrator/Application Developer	Scheme covering a target including an final business application. Targeted users are mainly Product/Application developers and integrators.
	Service Provider	Scheme covering a target including the platform or software as a service. Targeted users are mainly cloud (public/private) platform service providers.

Governance	Public	Governed by a public organisation
	Private	Governed by a private organisation
Certification Bodies	One	Has a single certification body (CAB)
	Several	Has multiple certification bodies (CABs)
Certification Validity	1 Year	Delivered certificates expires in 1 year
	2 Years	Delivered certificates expires in 2 years
	>2 and <5 years	Delivered certificates expires in 2 to 5 years
	Remains valid (with change management)	Delivered certificates do not expire by default but a surveillance and vulnerability management policies are enforced.
Certificate Maintenance	Yes	Includes a certification maintenance process
	Partially	Includes a certification maintenance process partially (some parts of the process are covered in other schemes)
	No	Does NOT Includes a certification maintenance process
Certificate Surveillance	Yes	Certificate Surveillance processes are defined
	No	Certificate Surveillance processes are NOT defined
Evaluation Costs	<5 K€	Evaluation cost less than 5,000€ in average
	>5K€ and <15K€	Evaluation cost between 5,000€ and 15,000€ in average
	>15K€ and <25K€	Evaluation cost between 15,000€ and 25,000€ in average
	>20K€ and <50K€	Evaluation cost between 25,000€ and 50,000€ in average
	>50K€	Evaluation cost over 50,000€ in average
Certification Costs	Free	No fees for Certification activities[10]
	<5 K€	Certification cost less than 5,000€ in average
	€>5K€ and <15K€	Certification cost between 5,000€ and 15,000€ in average
Regulatory Level	INTERNATIONAL	International laws, policies, and regulations apply
	EU	EU laws, policies, and regulations apply
	NATIONAL	National laws, policies, and regulations apply
	PRIVATE INDUSTRY (VERTICAL)	Private Industry policies, and regulations apply

[10] Certification activities cover mainly the evaluation report review and certificate issuance

C ANNEX: EU CYBERSECURITY ACT - ARTICLE 54: ELEMENTS OF EUROPEAN CYBERSECURITY CERTIFICATION SCHEMES

	Eu Cybersecurity Act - Article 54
(a)	subject-matter and scope of the certification scheme, including the type or categories of ICT processes, products and services
(b)	a clear description of the purpose of the scheme and how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme.
(c)	references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II of Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;
(d)	where applicable, one or more assurance levels;
(e)	an indication of whether conformity self-assessment of conformity is permitted under the scheme;
(f)	where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;
(g)	The specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 51 are achieved;
(h)	where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant;
(i)	where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;
(j)	rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;
(k)	where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;
(l)	rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;

(m)	rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;
(n)	where applicable, rules concerning the retention of records by conformity assessment bodies;
(o)	the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels;
(p)	the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;
(q)	the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes;
(r)	maximum period of validity of European cybersecurity certificates issued under the scheme;
(s)	disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;
(t)	conditions for the mutual recognition of certification schemes with third countries;
(u)	where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;
(v)	format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.

D ANNEX: TERMS AND DEFINITIONS

Abbreviation	Term
3GPP	3rd Generation Partnership Project
AAICR	Availability, Authenticity, Integrity and Confidentiality Requirements
AL	Assurance Level
CAB	Conformity Assessment Body
CAR	Cybersecurity Act Requirements
CC	Common Criteria (ISO/IEC 15408-18045)
CCMC	CEN CENELEC Management Centre
CEN	Comité Européen pour la Normalisation
CENELEC	Comité Européen pour la Normalisation Electrotechnique
CSA	Cloud Security Alliance
DG	Directorate General
EC	European Commission
ECCF	European Cybersecurity Certification Framework
ECCG	European Cybersecurity Certification Group
ECCS	European Cybersecurity Certification Scheme
ENISA	The EU Agency for Cybersecurity
ECC	European Cybersecurity Certificate
ECCVP	European Cybersecurity Certificate Validity Period
EN	European Standard
ESO	European standardisation organisation
ETSI	European Telecommunications Standards Institute
EUCA	European Union Cybersecurity Act
EUSC	European Union Statement of Conformity
FIDO	Fast identity online alliance
GP	Global Platform
IAA	International Accreditation Authority
IACS	Industrial Automation and Control System
IACSC	IACS Component

ICCP	IACS Cybersecurity Certification Process
ICCS	IACS Cybersecurity Certification Scheme
ICCEUR	IACS Cybersecurity Certification EU Register
IEEE	Institute for Electrical and Electronic engineers
IETF	Internet Engineering Task Force
ISMS	Information security management systems
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KPI	Key Performance Indicator
MB	Monitoring Body
MS	Member State
MSL	Member State Law
NAB	National Accreditation Body
NB	National Body
NCCA	National Cybersecurity Certification Authority
NCC	National Cybersecurity Certificate
NCCS	National Cybersecurity Certification Scheme
NIST	National institute of standards and technology
OASIS	Organization for the advancement of structured information standards
RQCS	Requirements of the Certification Scheme
PAS	Publicly Available Specifications
PP	Protection Profile
SC	Standardisation committee
SCCG	Stakeholder cybersecurity certification group
SDO	Standardisation Organisation
SO	Security Objectives
SP	Security Profile
TC	Technical committee
TCG	Trusted computing group
TD	Technical Domain
TestLab	Security Testing Laboratory
TR	Technical Report
TS	Technical Specification

TOE	Target Of Evaluation
UL	Union Law

TP-03-20-062-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-328-5
DOI 10.2824/481787