EUROSMART
The Voice of the Digital Security Industry

Cyber Resilience Act (CRA) - new cybersecurity rules for digital products and ancillary services

Eurosmart's feedback

Introduction

As underlined by President von der Leyen State of the Union 2021 address, the EU should become a worldwide leader in terms of cybersecurity. Cybersecurity is of utmost importance for the EU; it is at the same time a matter of European industrial policy, a provider of economic growth as well as an asset to gain the so-called "European digital sovereignty". In other words, cybersecurity has become a key marker of EU citizens' societal choice.

Through its last five years' initiatives, starting from the first NIS directive[1] as the first piece of EU-wide cybersecurity legislation, the European Union has been developing its regulatory instruments to ensure the cyber-resilience of the continent. The EU cybersecurity motto now favours collaboration with cybersecurity-leading countries over the initial EU decency on overseas' technologies. However, the Digital Single Market, whilst ensuring the free circulation of digital goods and services, doesn't provide any binding cybersecurity rules for placing digital products on the EU market. As a result, today, there is no guarantee that the digital product they have in their hands meets a minimum set of cybersecurity requirements for the end-users. The same approach applies to software and ancillary services: the Digital Single market lacks consistent requirements. The only way for the user to get consistent information about the security functions is to refer to the endless terms of services.

I. The EU Single Market lacks common baseline cybersecurity requirements

Clear and harmonised cybersecurity rules are definitively missing to ensure the proper functioning of the EU Single Market. This situation has a massive impact since digitalisation changes nearly every sector and their entire value chain. Moreover, the continuous development of digital products leads

[1] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

to an increasingly interconnected world. Whilst the capabilities of attackers are increasing, and due to a lack of common rules, the EU is expanding the surface attack of its internal market. The EU has already put in place some rules to regulate the cybersecurity of products and services. However, the current approach only covers a small part of the products placed on the market, mainly through the cyber aspects for radio-equipped online devices (Radio Equipment Directive)[2] while the main approach was on management systems for critical entities (NIS directive). The EU cybersecurity certification framework, as initiated by the Cybersecurity Act, is an excellent vector to address the cyber resistance of products, processes, and services to potential attacks, however, this interesting tool has not been activated to manage the market access and the market surveillance of ICT product, at best, this approach is limited to public procurements.

Even if tools have been created to tackle the cybersecurity aspects of digital products, the European Union is facing a regulatory gap in terms of mandatory and harmonised rules regulating cybersecurity for digital products. This situation leads to apparent drawbacks to European competitiveness when secure products cannot be the privileged choice of end-users.

2. CRA's should go beyond the NFL approach

2.1 The CRA needs a holistic approach towards cybersecurity

The European Commission's proposal for a Cyber Resilience Act is therefore much welcome by Eurosmart. The CRA should provide a holistic approach toward cybersecurity by complementing the current conformity framework established under the New Legislative Framework (NLF)[3]. However, the current EU conformity assessment framework seems too limited to concretely address cybersecurity aspects for digital products and ancillary services.

The CRA is expected to provide cybersecurity elements that are not managed through the current safety functional approach; for instance, the CRA would be able to

- Guide manufacturer on the risk classification of their products.
- Address the entire life cycle of Digital products and their ancillary services.
- Anticipate the potential unintended misuse of products and ancillary services.
- Evaluate the robustness of digital products and the tamper resistance to potential attacks.

  Support securing personal data including Personal Identifiable Information (PII) when they are generated, stored, processed, or transferred by digital products and ancillary services. A link with GPDR certification could be established.
- Support securing data pertaining to digital products. (e.g. traceability of versions and updates, authenticity check).
- Provide the market-surveillance authorities with additional competences in cybersecurity, which comes along with the obligation of the vendor to disclose and mitigate identified vulnerabilities and stepwise recall mechanisms.

[2] The Delegated Regulation EU 2022/30 defines requirements in the area of cybersecurity for products covered by the RED. This concerns in particular sections d) to f) of Article 3.3:

[3] Requirements for accreditation are set in Regulation 765/2008

2.2. Shortcomings of the safety approach

The goals and values of safety and security are in some places contradictory. In the field of classic safety, functions are enabled in potentially dangerous machinery to protect people and the environment. When it comes to security, however, the objective is not to protect people from machines. Cybersecurity will consider if the machine is enough robust so that people can’t bring it to an unexcepted behaviour or switch off relevant security functions. If such situation happens, mitigation measures should be put in place.

In the context of security, the risk management is more directive. It is a matter of dealing with attackers who have means and clear interests. Safety will instead be more considering errors or incidents. These distinctions require the use of a third-party service for Digital products security assessment. Moreover, unlike the NLF, a risk analysis cannot be delegated to manufacturers and developers.

Since the applicable requirements are not the same for safety and cybersecurity, Eurosmart recommends the legislator to set up clear definitions for these respective domains.

2.3. The NLF modules stick to functional security

To place products on the EU market and assess their conformance to essential requirements that guarantee their "safety", the NLF defines a horizontal menu of conformity assessment modules, and the NLF sectorial legislation selects the most appropriate ones according to the level of protection desired. This assessment of the risk associated with given product results from a compromise between the adequate level of security and an evaluation procedure that remains less constringent for the manufacturer. This module approach is not sufficient to seriously address cybersecurity risks; the assessment provided remains static and only focuses on the product's correctness.

Based on the Radio Equipment Directive requirements that cover some digital security aspects, the following NLF modules[5] could be activated to leverage a risk classification:

Tab. 1 List of NLF modules to support the CRA

Type of modules	Type of assessments
Module A (Internal production control),	The legislation could allow vendor's self-assessment for limited risk
Module B (EU-type examination) and **Module C** (Conformity to EU-type based on internal production control) Or **Module B** (EU-type examination) and **Module D** (Conformity to EU-type based on quality assurance of the production process)	The legislation requires a third-party assessment, the vendor selects the relevant modules
Module H (Conformity based on full quality assurance)	The legislation requires the involvement of a third-party assessment, the vendor selects the relevant modules

[5] The ‘Blue Guide’ on the implementation of EU products rules 2016 - Section 5.1. Modules for conformity assessment. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016XC0726%2802%29

Caption: *Although these modules address both design and production phases, cybersecurity requires considering the whole product life cycle in a dynamic environment. What is true when the product is assessed and placed on the market might be different in the future due to the evolving nature of the Digital Product.*

Whatever the choice of the module is, due to the limitation on design and production phases and the focus on functional security, a large part of cybersecurity functionalities is not covered. Hence, this selection cannot be considered as a sufficient risk-based approach by the legislator.

Moreover, even for module H, which considers a conformity based on full quality assurance, many aspects are in fact performed in-house by the manufacturer. The third-party assessment for module H does not apply to the overall evaluation process.

The choice of modules is more related to a level of assurance rather than ta level of risk to be covered. This solution is clearly not suitable for cybersecurity assessment. Addressing cybersecurity in a such way would increase the surface attack of interconnected Digital products. Risk assessment remains key; therefore, the legislator should be prescriptive by defining a suitable framework for risk assessment. Moreover, the complete review and assessment should be performed by a sole third party.

3. The CRA need a risk-based approach based on the European Cybersecurity Certification framework

To achieve its objectives, the CRA should provide a risk-based assessment framework with several assurance levels according to the identified risks. Moreover, the framework must consider the entire life cycle and changes in the threat landscape. Eurosmart believes that NLF should be adapted to cover this aspect for these reasons. However, according to the better regulation approach, the legislator should best use the already existing legislative instruments. In this respect, the European Cybersecurity certification framework, as defined by the Cybersecurity Act (CSA)[6], provides interesting elements that could be used for market access (e.g. cybersecurity evaluation) and market surveillance purposes (e.g. vulnerability disclosures and mitigation measures). Eurosmart recommends the Commission consider bridging between the NLF and the CSA; the CRA deserves to be linked with the EU Cybersecurity certification framework.

Cybersecurity evaluation is a matter of moving targets to anticipate the intent of attackers, where risk is defined as a mix of impact and probability according to the intended use and the environment of the product. Moreover, cybersecurity is considered a dynamic environment where attack methods, threats, and functionality of products and services evolve over time. The purely functional product safety approach of the current NLF cannot encompass all these cybersecurity aspects. The result of the CRA cybersecurity assessment should make sure that the product is robust enough to resist to potential attacks in such a dynamic and evolving environment. Therefore, to achieve this goal, a third-party assessment according to an evaluation methodology is necessary.

Hence, the provisions of the CSA can play a key role: the risk-based approach provided by certification schemes models is fully designed to demonstrate the fulfilment of Cybersecurity requirements.

[6] Regulation (EU) 2019/881 – Cybersecurity Act

Tab. 2 Comparison between NLF and CSA

	Cybersecurity Act		New Legislative framework	
Security levels	Means	Type of assessment	Means **	Type of assessment
BASIC* Compliance against "essential requirements"	EU Scheme basic	Conformity Self-Assessment	Module A – Internal production control	Self-Assessment
	EU Scheme Basic	Certificate basic – Conformity assessment body	Module B+C, or B+D Assessment of individual product (type) and production	In house conformity assessment body Or Third party
			Module H *** Assessment of "Full Quality Assurance System"	Third Party (partially)
Substantial Security functions enable to minimise the known cybersecurity risks	**EU Scheme** "Substantial"	Certificate Substantial – Conformity assessment body	****	
High Security functions at the "state-of-the-art", the product is pentested	EU Scheme "High"	Certificate High – National Cybersecurity Certification Authorities	****	

Caption: *Compared to the CSA, the NLF is not covering the full cybersecurity spectrum:*

** Basic security level could be reached through NLF modules and the CSA at the same time*

*** NLF modules provide a discretionary risk assessment which is not fully completed by a neutral third party. This is a limiting factor to fully assess the robustness of the Digital products.*

**** Module H is not a full third-party assessment; some aspects are directly managed by the vendor. This module is not suitable for a substantial security level.*

***** NLF does not consider substantial and high levels.*

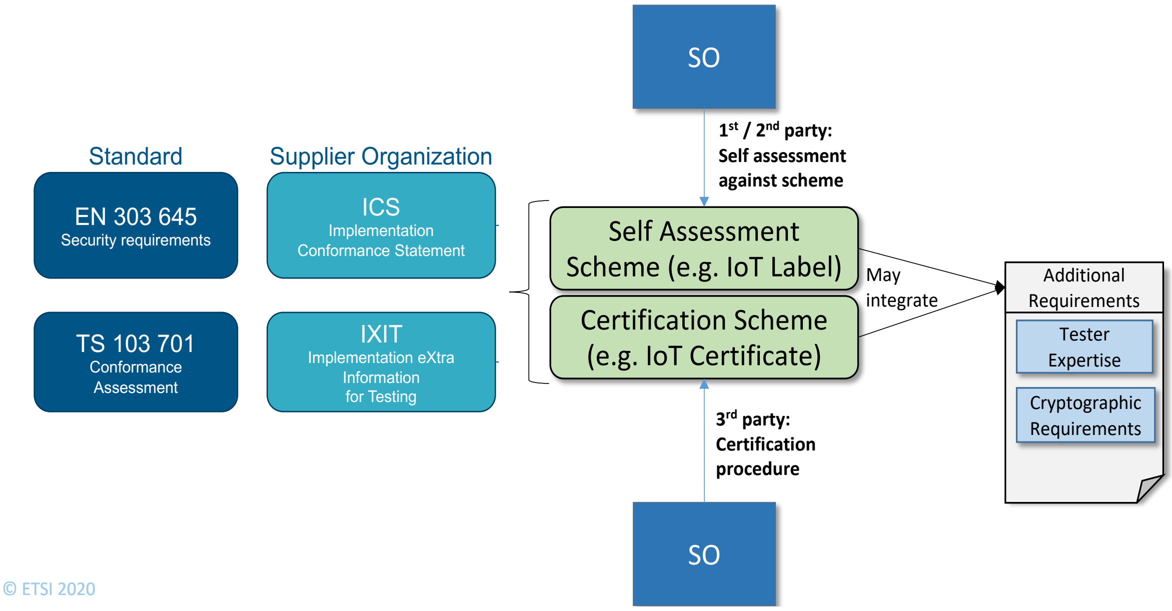
Basic security requirements could be fulfilled at the same time through NLF modules and the CSA

The security level « basic » could be reached though the NLF modules by complementing the current safety compliance perimeter with additional cyber security requirements.

The selection of modules remains relevant and flexible to tackle basic cyber-security targets for basic baseline security requirements, such as cyber hygiene processes. For these basic digital products, which cybersecurity functions are not critical for the market access, as for the NLF, the CRA should allow the vendors to select the most appropriate option between a self-declaration based on harmonised European standards or assessment of conformity to the market surveillance authorities and a third-party evaluation. In any case, this first basic level cannot be considered as a cybersecurity evaluation but as a proof of functional security at a given time. For instance, module H standing for conformity based “full quality assurance” is not a complete assessment by an independent third party.

In parallel, the CSA could answer to basic security requirements as well. The CSA provides 2 options: a conformity self-assessment and a conformity assessment carried out by a Conformity Assessment body (CAB). Existing security standards such as ETSI EN 303645 / TS 103701 could support a future self-assessment scheme or a third-party assessment against the level “basic".

Fig. 1 Mapping of EN 303645 / TS 103701 on self-assessment schemes and future CSA IoT schemes



***Caption:** CSA “basic” can provide a “declaration of conformity” or a “certificate”. As part of the scheme a label could be added. (source ETSI).*

3.5. Digital products should be evaluated against CSA's assurance level "Substantial "

A big portion of digital product will have an associated risk beyond ‘low risk’ while they are not being mapped to to ‘medium risk’. While the NLF does not reflect this approach the CSA takes the associated assurance level ‘Substantial’ into account.

3.1. Critical Digital products should be evaluated against CSA's assurance level "High"

The cybersecurity act provides that other (vertical) EU legislation can rely on European cybersecurity schemes to assess the robustness of specific products. It is important to ensure consistency with the other bricks of legislation and precisely when they concern the CSA assurance level "High". Most of the critical building blocks and other "essential requirements" of the upcoming piece of legislation are expected to rely on such level of assurance.

Moreover, critical digital product deserves to be resistant to skilled attackers: penetration testing relying on maintained attack method and catalogues are the only way to confirm that a given digital product has reached the state-of-the-art. These tests often require a "white box" approach; the source code of the digital product is provided to the evaluator; since this approach is highly critical, and as prescribed by the Cybersecurity Act, Eurosmart recommends relying on NNCAs to perform these tests.

In addition, the NFL established the European Accreditation, meaning that recognised third countries’ laboratories can perform security tests. Since critical security level requires access to digital product source codes, this situation may lead to a breach of digital sovereignty.

To conclude, the current NLF framework has not been designed to perform the cybersecurity evaluation of these types of products. Therefore, the CRA should rely on the European Cybersecurity Certification framework.

4. The CRA should enable Composition Certification

To mitigate cybersecurity risks various cybersecurity features, need to be implemented and maintained in order to reduce associated risks. The cost effectiveness of assessments can be optimized by using already existing assessments as a general principle.

The Cyber Resilience Act should also support the cyber resilience on system level. Composite certification is an understandable means not only for manufacturer but also for operator of products and services.

5. Digital products’ Labelling

Looking at the EU energy label efficiency class, Digital product labelling could be a helpful element in raising end-user's awareness of digital product cybersecurity functions. The Cybersecurity Act provides cybersecurity labels for certified products that could ensure more transparency, especially for consumers[7]. This label is bound with the deliverance of an EU cybersecurity certificate or an EU

[7] Regulation (EU) 2019/881 – Cybersecurity Act art. 54

statement of conformity; it provides clear information on the assurance level reached by the digital product. This information is maintained and provided by ENISA as a trusted independent and public body. This label is also an incentive for producers and developers who can refer to this label to advertise their products.

The label starts as of level of assurance basic; it could be a complementary or an alternative approach to the current NLF conformity assessment. For digital products that do not require advanced security functions, the producers and developers may choose between the CSA' basic' including a label or the traditional NLF safety approach.

6. Software should be considered as a Digital product

6.1 The digital single market lacks security requirements for software

Software solutions are entirely part of our daily lives, and their malfunctioning can modify the expected behaviour of a device and lead to significant damage. Cybersecurity is a matter of trust; as for hardware devices, the CRA should provide what and who guarantees the level of confidence in the security of the software. In most cases, software security is ensured in a reactive mode; to get an idea of the robustness of software, the user can only refer to incident notifications which concern vulnerability disclosures. The framework is mainly provided by the NIS directive and the CERT EU framework[8]. Browsing the list of vulnerabilities and incidents remains the only way to measure this level of security.

Therefore, the legislator should establish clear rules for placing software on the market and consider the latter as a digital product. The CRA should encompass several requirements to make sure that software placed on the market are :

- Safe (from a functional approach) as any other goods placed on the EU market
- Cyber-secure means that relevant security functions have been put in place and will be efficient enough to resist potential attacks over time.
- Free of backdoors.
- Respecting and protecting personal data and complying with the EU principle of privacy as stated by art 8 of the EU Charter of fundamental rights.
- Acting in a manner, they do not threaten or put at risk other software or associated data.

The classification of software as a Digital product should come along with liability. The CRA should provide full liability to the developer, as it is the case with any products placed and purchased in Europe. The situation where the sole hardware manufacturers assume the full liability of compromised devices due to a software failure will be highly detrimental to the market.

6.2 The CRA should require software methodology development and life-cycle management

Security functions and requirements will vary according to the type of software and its environment. According to a risk-based approach, the legislator should provide a clear definition of software falling

[8] Directive (EU) 2016/1148 - art.16 “Security requirements and incidents notifications” https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN#d1e1775-1-1

under the CRA. According to the software criticality, the CRA should define the minimum set of security functions. To achieve this set of goals as the minimum and comparable requirements, different types of software won't follow the same development methodology. Still, they must embed security into their secure software development life cycle to avoid becoming an easy target for hackers. The guarantee that the security functions are correctly enabled chiefly relies on how security is embedded into the development methodology (Agile, DevOps, waterfall, Rapid Application development etc.).

The current state of play does not provide a coherent and comparable approach for the EU market. Therefore, to assess the software as any other product, an EU recognised evaluation methodology for SDLC is necessary.

Once again, the Cybersecurity act is an interesting tool to explore. According to the definition provided by the legislator, the development of EU cybersecurity schemes for software would guarantee that the security functions have been correctly implemented. Moreover, EU cybersecurity schemes are the right tool to address the vulnerability disclosure and the obligation to mitigate them.

7. CRA Risk classification and Evaluation Methodology

To properly evaluate the digital product according to the risk associated, the CRA should reference a generic risk classification.

Recall: safety risks and security risks.

A products-centric approach should consider various use cases and situations which are associated to different risks being mapped to different risk levels. Therefore, various risk dimensions and risk spectra, including functionality, connectors, complexity, application, intended use, data flows, environment, societal and individual impact, etc. should be taken into account. The associated vertical regulations may refine this approach according to specific use cases.

EU certification scheme relies at the same time on functional security requirements and certification methodology. This methodology could be used for a large category of products by developing specific functional security requirements. To cover the so-called "essential requirements", the CRA should support the development of functional standards.

8. Enhancement of the market surveillance rules to address cybersecurity

The NLF provides a framework for market surveillance (ref). It established rules to appoint a National accreditation body. However, this framework does not consider the whole product life cycle. Mandatory updates and vulnerability disclosures and the obligation to ensure mitigation of known vulnerability are missing today. Eurosmart considers that such market surveillance obligation must be put in place through the CRA to establish a duty of care. Once again, the Cybersecurity act is fundamental: National accreditation bodies should identify National Cybersecurity Certification Authorities (NCCAs). These public entities have the capability to manage market surveillance mechanisms for cybersecurity aspects. NCCAs are already collaborating for EU cybersecurity schemes' maintenance through the already established European Cybersecurity Certification Framework (ECCG), where NCCAs and relevant public authorities from all Member states are represented.

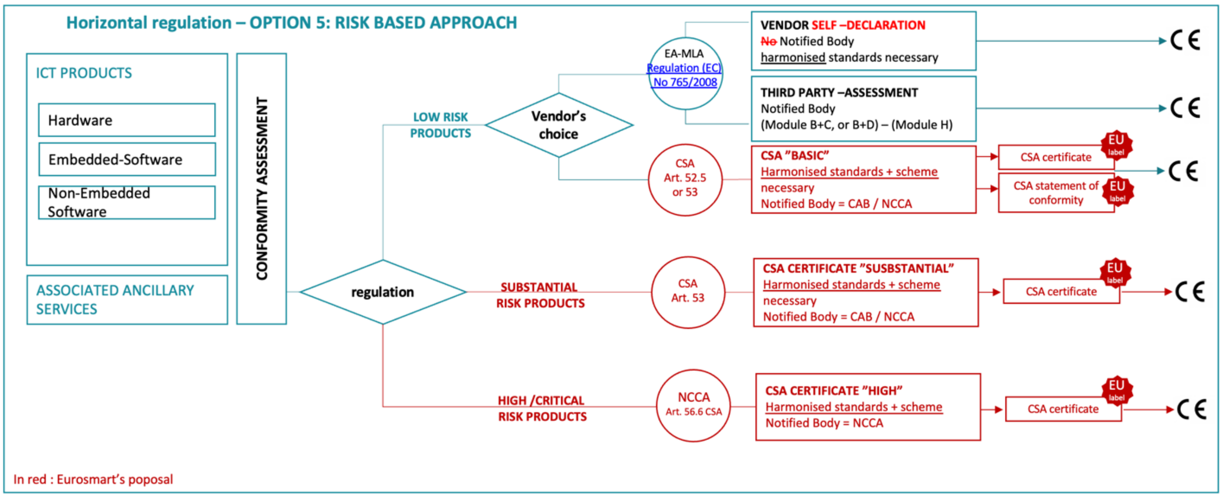
To address the complete life cycle of digital products, the CRA should grant market surveillance capabilities to the NCCAs, and more specifically, when it comes to vulnerability management and the obligation to mitigate these risks[9]

In addition, the NCCAs have been designed and have the relevant knowledge to supervise the Conformity Assessment Bodies[10] that have been appointed pursuant to Regulation (EC) No 765/2008.

An important part of market surveillance are associated mechanisms like the Recall mechanism for unsafe devices. Currently there is no mechanism in place to handle vulnerable digital products already placed in the market. A stepwise approach would give guidance to manufacturer and citizen.

Conclusion

Fig. 2 Eurosmart's proposal


Horizontal regulation – OPTION 5: RISK BASED APPROACH
ICT PRODUCTS
Hardware
Embedded-Software
Non-Embedded Software
ASSOCIATED ANCILLARY SERVICES
CONFORMITY ASSESSMENT
regulation
LOW RISK PRODUCTS
Vendor's choice
EA-MLA Regulation (EC) No 765/2008
VENDOR SELF –DECLARATION
~~No~~ Notified Body
harmonised standards necessary
THIRD PARTY –ASSESSMENT
Notified Body
(Module B+C, or B+D) – (Module H)
CSA Art. 52.5 or 53
CSA "BASIC"
Harmonised standards + scheme necessary
Notified Body = CAB / NCCA
CSA certificate
CSA statement of conformity
EU label
SUBSTANTIAL RISK PRODUCTS
CSA Art. 53
CSA CERTIFICATE "SUSBSTANTIAL"
Harmonised standards + scheme necessary
Notified Body = CAB / NCCA
CSA certificate
EU label
HIGH /CRITICAL RISK PRODUCTS
NCCA Art. 56.6 CSA
CSA CERTIFICATE "HIGH"
Harmonised standards + scheme
Notified Body = NCCA
CSA certificate
EU label
CE
In red : Eurosmart's poposal

Caption: *The CRA should define a risk-based approach and rely on EU cybersecurity schemes to complement the current NLF functional security approach.*

Eurosmart fully supports the CRA general objective but would recommend a scalable approach for both hardware and software products. The CRA should clearly define the type of products falling under its scope since the market access and market surveillance rules are closely bound with liability. A clear definition of cybersecurity is missing: the resistance of a given product to potential attacks cannot be guaranteed through a functional approach. Moreover, the current NLF has been designed to address functional security requirements only, which do not cover the full spectrum of cybersecurity. Therefore, additional security elements must be considered, such as resistance to potential attack, vulnerability disclosure, patch management and other mitigation measures. To achieve this goal, and in addition to the NLF conformity framework, the European cybersecurity certification framework should be used. From this stance, the CRA cannot avoid on developing new functional security standards alongside certification methodology to concretely assess the cybersecurity level of the digital products placed on the market.

[9] Regulation (EU) 2019/881 – Cybersecurity Act art. 58. 7 (a).
[10] Regulation (EU) 2019/881 – Cybersecurity Act art. 58 7 (f) and (g)).

Annex I: CSA assurance levels

Cybersecurity Act	
Assurance Level	Type of assessment
Level Basic At least review of the technical documentation	Conformity self-assessment – EU statement of conformity
	EU cybersecurity certification schemes could provide for a conformity assessment to be carried out under the sole responsibility of the manufacturer or provider of ICT products. Applicable for low complexity ICT products with low risk to the public
	European cybersecurity certificate basic
	Conformity Assessment Body
	The CA procedure is carried out by an independent private third party (accredited conformity assessment body). to minimise the known basic risks of incidents and cyberattacks
	European cybersecurity certificate 'Substantial'
Level Substantial	Conformity Assessment body
Security functionalities to minimise the known cybersecurity risks	Evaluation to be performed by an accredited CAB. It should assess security functionalities to minimise the known cybersecurity risks, to address the risks of incidents and cyberattacks carried out by actors with limited skills and resources and no public-known vulnerabilities
	European cybersecurity certificate 'High'
	NCCA
Level High Pentesting	Evaluation to be performed by an NCCA It should assess security functionalities to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources and no public-known vulnerabilities. Penetration testing mandatory.

Annex 2: Applicable NLF modules for Digital products

New Legislative Framework		
Assurance level		Type of assessment
Module A – Internal production control (full application of harmonised standard)	Map the level of risk	Self-Assessment
		No Third-party involvement in the CA A declaration accompanied by the relevant technical examination and documentation of the manufacturer is enough to ensure the conformity of the product

Module B+C, or B+D Assessment of individual product (type) and production Module H Assessment of "Full Quality Assurance System"	Map the level of risk	Declaration of conformity
		In house CA-Body
		The CA is performed with the involvement of an accredited in-house CA body that forms a part of the manufacturer's organisation.
		External conformity Assessment body
		The CA is performed with the involvement of a third-party: an external conformity assessment body