EUROSMART
The Voice of the Digital Security Industry

Cyber Resilience Act

Eurosmart's feedback

Introduction

Over the last decade, the European Union has been developing a solid cybersecurity regulatory approach. The overall approach is to make the European market more resilient while ensuring the digital sovereignty of the whole continent. This trend has prioritized sensitive domains that deserve strong resilience to more and more skilled attackers. At the same time, a large number of regulatory compliance requirements in the area, or with components on cybersecurity have been developed. Bringing potential confusion and over-regulation to the market. Hence the need for a horizontal minimum set of cybersecurity requirements is necessary.

Eurosmart has identified key topics to be considered while examining the draft legislation:

I. Interplay with existing policy provisions

Eurosmart acknowledges and praises the effort of the commission to identify cyber security policies that intersect with the proposal from the Cyber Resilience Act. This is a point of great interest to the industry to reduce fragmentation, and overregulation, drive adoption, reduce friction, and achieve a more cyber-resilient European market.

Some areas need further refinement:

I.1. Reasons for and objectives of the proposal

Eurosmart wants to call to the attention of the commission that while the objectives are clearly defined in the introduction, the regulation identified as "Resilience" does not acknowledge the entire resilience stack[1]:

- Protection – Identified under the essential cybersecurity requirements (Annex I)
- Detection – Addressed by the vulnerability and patch management (Annex II)
- Recovery – Neither acknowledged nor recommended.

This last element of resilience, recovery, is addressed and encouraged by the NIS Directive [Directive 2016/1148]. While components of the recovery are addressed in the form of the possibility to reset the product to its original state and patching support, Annex I. sections 1.3(a) and 2(8), it isn't an integral part of the Resilience Act, Eurosmart recommends a revision of the text to include this language and when appropriate, indicate this element will be covered by the NIS Directive. As this will enhance visibility and capability about products with digital elements providing the three elements of recovery in cybersecurity, aligning with the EU commission objectives around the "Better Regulation" approach.

I.2. Reporting cyber incidents.

The GDPR [Regulation 2016/679] and the NIS Directive [Directive 2016/1148] have both reporting obligations for cyber incidents, including vulnerabilities. Given the fact that data breaches can be the product of actively exploited vulnerabilities, Eurosmart believes in aligning the requirement since none of those policies aligns with the CRA proposal, as expressed in Article 11.2. Moreover, Eurosmart recommends a 72 hour-window for manufacturers reporting cyber incidents.

I.3. Security for privacy

The GDPR [Regulation 2016/679] identifies elements under the CRA scope as it is the case of cybersecurity of data in transit and at rest, as well as data encryption. For those elements of conformance, guidelines need to be established and Eurosmart recommends the commission to align the interpretation of conformance, under GDPR for CRA conformant products in alignment with the EDPB[2].

This scenario is manifest in the requirements from Annex I, 1. (3)(b), 1. (3)(c) and 1. (3)(e) and its applicability in the context of the GDPR and the CRA proposal. It is unclear if a product compliant to

[1] "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations", NIST Special Publication 800-171, Revision 2, Ron Ross, Victoria Pillitteri, Kelley Dempsey, Mark Riddle, Gary Guissanie. February 2020

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

[2] Recital (16) of the CRA proposal

annex I under article 24 or article 18 is considered compliant with the provisions of GDPR relating to those aspects, as well as the demonstration of conformance to these points to the GDPR supervision authorities. Leaving open the possibility for an overlap in supervision: the one brought by GDPR and the current CRA text proposal.

The ePrivacy Directive 2002/58/EC, indicates "Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users.". Article 14 refers to "**Technical features and standardisation**", suggesting in section 3: "*Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, following Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications*."

Eurosmart invites the commission to qualify and advise on the applicability and relation of the CRA conformance for conformance with the ePrivacy directive, and to provide guidance in the interoperability between the common requirements for terminal equipment considered as a device with digital elements.

1.4. Security for safety

There is no safety without security. Therefore, the General Product Safety Directive (GPSD) [Directive 2001/95/EC], and its relation to CRA Article 7, must be qualified and aligned.

Under the revision, the liability act, Directive 85/374/EEC doesn't necessarily align the definition of product with the usage of "digital elements", nor it's consistent with the support and obligation of vulnerability handling on the manufacturer side defined by the CRA Article 10.6 as 5 years (at most), while it's 10 years by the liability act proposal. Also, the definition of cyber incidents and the potential recall when they are considered quality incidents doesn't reflect the criteria for recall scenarios as presented under the CRA [Recital (16) CRA proposal].

1.5. Consistency with the AI act.

Eurosmart wants to bring to the attention of the commission points where additional clarification from the commission is required in the context of the CRA implementation for high-risk AI systems:

- Article 8.1, refers to a "level of protection" which is not defined or established in the document.
- Article 8.2, it is stated that the conformity procedure as required by article 43 shall apply to cybersecurity requirements:
    - The equivalence of the conformity assessment procedures described in article 43 and article 24 is not obvious as they are described in different ways. How can manufacturers be sure that they provide the same level of trust regarding cybersecurity requirements?
- Article 8.2, for clarity, the following wording "[…] provided that the compliance of those notified bodies with the requirements laid down in Article 29 of this Regulation have been assessed […]" should be replaced as follows: "[…] provided that the compliance of those notified bodies with the requirements laid down in Article 29 of this Regulation is fulfilled […]".

    - This point is important as the applicable requirements for notified bodies are different (e.g. under the CRA they shall be established under national law, which is not required in the AI act)
- Article 8.3, What is the scenario when the conformity procedure based on Annex VII is used?
    - Does it mean that such a procedure is acceptable to demonstrate conformity with cybersecurity requirements? In that case, how can manufacturers be sure that such an approach provides the same level of trust as the provisions of Article 24(2)(a), 24(2)(b), 24(3)(a) and 24(3)(b)? The provisions of this text shall apply when the conformity procedure based on Annex VI is used AND ALSO when the conformity procedure based on Annex VII is used.
- What if an AI system also falls into the highly critical product category? It seems [AI act] article 43 does not allow for a mandatory CSA certification….It would lead to the situation where the conformity assessment of an AI system classified as highly critical would be carried out without relying on a CSA security certificate but rather relying on a module (B+H) like approach, while CSA certification would be mandatory for a highly critical product fully falling under the current text. This creates a loophole in the overall security of highly critical products.

1.6. Consistency with the RED requirements

The activation of the articles of the RED dealing with cybersecurity requirements is the first attends to address cybersecurity market compliance namely: 3(3)(d), to ensure network protection; 3(3)(e), to ensure safeguards for the protection of personal data and privacy; 3(3)(f), to ensure protection from fraud.

This approach remains restricted to certain types of products with a radio connection to the internet. The CRA's approach is transversal.

There is an overlap between RED cybersecurity requirements - 3(3)(d), to ensure network protection; 3(3)(e), to ensure safeguards for the protection of personal data and privacy; 3(3)(f), to ensure protection from fraud - and the CRA requirements laid down in Annex I.

- The EC has requested the development of harmonized standards
- RED harmonized standards will be designed for “self-declaration of conformity”

CRA art 20.3 provides that a single EU declaration of conformity shall be drawn up in respect of all Union acts. However, critical products with digital elements (and especially class II) require a third party-assessment. Hence, new harmonized standards and methodologies should be drawn up to cover the same requirements. RED harmonized standards would become obsolete for many products.

Moreover, the lifetime for RED harmonized standards would be very short for many products. This hEN development requires many efforts and would be applicable as of the 1st of Aug 2023 till the implementation of the CRA. This could potentially generate ambiguity on what the type of approval represents since the criteria seem to be changing even before starting.

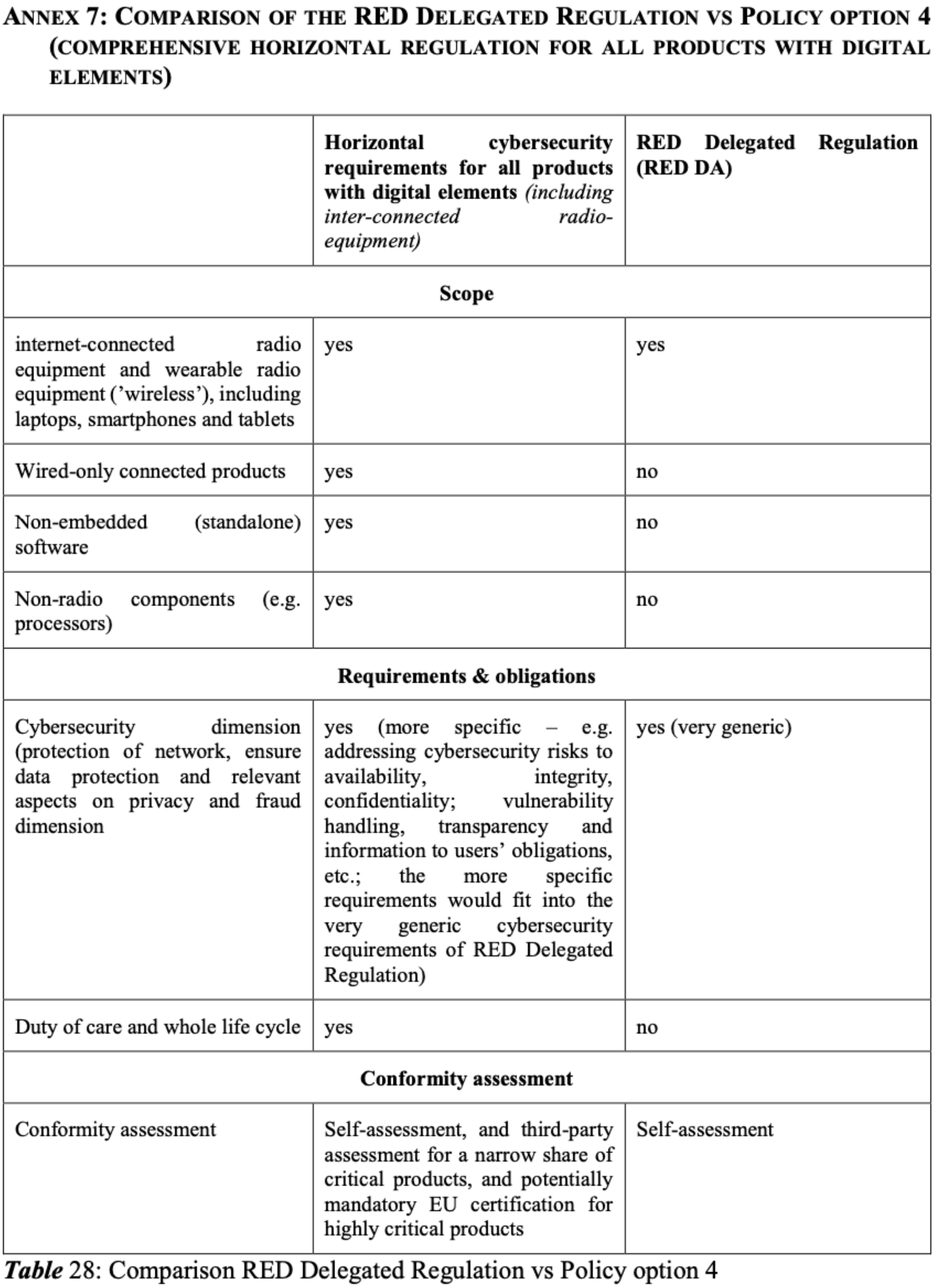
As recital (15) acknowledges RED hEN as the potential base for a new set of CRA hEN, Eurosmart recommends having a clear position from the commission either to hold or amend RED hEN developments in consideration of the CRA proposal.

With regards to Article 3(3)(i) activation, software updates, this is not yet activated by RED but in the scope of CRA. This generates confusion as to what is on the scope of conformance among those regulations. The recommendation from Eurosmart to the commission uniformity with RED aligns the terminology and criteria for type conformance among CRA and RED considering the status the Article 3(3)(i) activation.

The narrow correspondence between the RED and the CRA is reflected in figure 1, a reproduction of table 28, in Annex 7, from the comparison of the RED delegated regulation vs policy option (comprehensive horizontal regulation for all products with digital elements), EC 15.9.2022 SWD(2022) 282 final[3].

The RED is expected to provide more generic cybersecurity requirements reflected in the hENs following the RED DA on 3(3) d-f. There is no comparison included so far on the respected Risk Assessment which of the RED, the hENs are based on, concerning the Risk assessment expected to be provided related to the CRA hENs. In this aspect, Eurosmart recommends alignment where feasible.

[3] https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2022)282&lang=en



ANNEX 7: COMPARISON OF THE RED DELEGATED REGULATION VS POLICY OPTION 4 (COMPREHENSIVE HORIZONTAL REGULATION FOR ALL PRODUCTS WITH DIGITAL ELEMENTS)

	Horizontal cybersecurity requirements for all products with digital elements *(including inter-connected radio-equipment)*	**RED Delegated Regulation (RED DA)**
Scope		
internet-connected radio equipment and wearable radio equipment ('wireless'), including laptops, smartphones and tablets	yes	yes
Wired-only connected products	yes	no
Non-embedded (standalone) software	yes	no
Non-radio components (e.g. processors)	yes	no
Requirements & obligations		
Cybersecurity dimension (protection of network, ensure data protection and relevant aspects on privacy and fraud dimension	yes (more specific – e.g. addressing cybersecurity risks to availability, integrity, confidentiality; vulnerability handling, transparency and information to users' obligations, etc.; the more specific requirements would fit into the very generic cybersecurity requirements of RED Delegated Regulation)	yes (very generic)
Duty of care and whole life cycle	yes	no
Conformity assessment		
Conformity assessment	Self-assessment, and third-party assessment for a narrow share of critical products, and potentially mandatory EU certification for highly critical products	Self-assessment

Table 28: Comparison RED Delegated Regulation vs Policy option 4

Figure 1.

1.7. The Chip Act

Chips and in general semiconductors are a special resource in almost all fields. They are special since they are a key element for the security of end devices. They typically do not operate “alone” but rather in composition, so their operation environment adds to the security of the products. They are also particular items since customers of semiconductor products are very sensitive to supply chain interruptions. Therefore, it makes sense to treat chips horizontally and in the same way independently of the field of application. Furthermore, European semiconductor vendors have to participate in worldwide competition while players from other parts of the world can “leave out” the European market or take shortcuts if rules cannot be enforced.

In the opinion of the Eurosmart members, given that semiconductors are listed as products in the scope of the regulation as per Annex III, CRITICAL PRODUCTS WITH DIGITAL ELEMENTS, Class I and II, the omission of the Chip Act proposal is notable. Moreover, considering that the Chip Act itself refers to a standardization effort for trusted chips, that in spirit mirror the goals of CRA covering the whole life cycle of products and conformity assessment procedures: *The commission will work with Member States and private actors to identify sectorial requirements for trusted chips to establish common standards and certification, as well as common requirements for procurement, to be developed with the support of the European standardisation organisations where appropriate and bearing in mind the principles of the New Legislative Framework for conformity assessment and market surveillance*[4].

Given the nature and complexity of the silicon assessment topic and the ongoing activities as part of the Chip Act where conformance requirements will be defined for such kinds of products, it might be reasonable to consider potential scenarios:

- Recognition of CRA conformance for Chips certified under a CSA scheme through delegated act as expressed in Article 18.3 of the CRA proposal.
- Recognition of CRA conformance for Chips certified under a Chip Act standard developed by an ESO.
- Recognition of conformance employing a joint CRA-Chips Act standardisation mandate to ESOs to ensure the compliance of both texts.

Eurosmart recommends the commission consider adopting the development of standards for Trusted Chips under the scope of the Chip Act as the mechanism to show conformance with the CRA requirements. This will allow CRA to prioritize end devices while addressing the CRA objectives for Trusted Chips in a matter-expert (*lex specialis*) forum. It helps limit the scope and prevent over-regulation of the semiconductors and related IP products like Secure Crypto-processors listed in Annex II, Class III of the proposal.

[4] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0046

2. Relation with the EU CSA (2019/881)

2.1. Security for Resilience

Article 18.4 from the CRA proposal activates the mechanism to show conformance with the essential requirements using the certification of products with digital elements with schemes adopted under Regulation (EU) 2019/881, Cyber Security Act (CSA). Eurosmart welcomes this approach as an example of building European cyber resilience by adopting products with certified security capabilities.

Under Article 18.3 on "Presumption of conformity" and EU cybersecurity Schemes, CRA provides a risk-based approach established under a predefined list of products (which could be updated time-to-time). The CRA is not dealing with Levels of Assurance. Instead, it addresses the level of criticality through in-house or third-party assessment.

When identifying or mandating EU cybersecurity schemes as means to demonstrate compliance with CRA requirements, Eurosmart recommends the commission increases the transparency on how the assurance(s) level(s) will be applied. The relation between levels "basic", "substantial", and "high" in the context of CSA and its applicability for CRA Class 0, Class I, Class II and highly critical products.

Moreover, schemes would evolve, and scheme maintenance mechanisms should be established. This leaves open for clarification of the implication of considering the EU schemes' compliance with the CRA requirements when updates occur. At the present, there are no CSA schemes applicable for CRA conformance. The European Common Criteria Scheme in EUCC will be, for the foreseeable future, the main scheme available for demonstrating conformance with CRA and in the context of this text, EUCC is used as reference.

Eurosmart recommends clarifying the governance model when CSA schemes are used as proof of conformance as there is a need to liaise with SCCG, as ECCG identifies these schemes and ensures their maintenance with stakeholders' support (e.g., ISAC). In this respect, when it comes to Class 0 (non-critical products), which would represent 80% of the market product products, a clear link should be established with basic-level European cybersecurity certificates and a CSA statement of conformity. Future European schemes would cover most of these products, therefore Eurosmart encourages the legislator to leverage the CRA to facilitate the adoption of the CSA basic level.

Eurosmart wishes to contribute by elaborating on the elements of conformance for different product types and suggesting the commission review and elaborating on the contents from tables 1 to 4.

Type of conformity assessment	Class 0 "Products with digital elements" which are not high-risk AI systems	Class 0 "Products with digital elements" which are high-risk AI systems Conformity assessment procedure as defined in AI act art. 43 applies.
Presumption of conformity Harmonized standards (art 18.1) Common specifications (art 18.2)	✓	✓
Internal control procedure (based on Module A)	✓ Possible (art.24.1)	✓ Where harmonized standards or common specifications have been used, procedure similar to module A.
EU-type examination procedure (based on module B) set out in Annex VI followed by ***conformity to EU-type based on internal production control*** (based on module C)	✓ Possible (art.24.1)	✗ N/A
Conformity assessment based on full quality assurance (based on module H)	✓ Possible (art 24.1)	✓ Procedure similar to module H.
(EU) 2019/881 ***EU statement of conformity – Self Assessment*** [Basic CSA art.53] or ***certificate issued by a CAB or NCCA*** [Basic, Substantial and High CSA art.60]	✓ By implementing act to identify eligible CSA scheme to demonstrate conformity (art 18.2)	N/A

Table 1: Type of conformity assessment for products in Class 0

Type of conformity assessment	**Class I** **“Critical product with digital elements” (Annex III) which are not high-risk AI systems**		**Class I** **“Critical product with digital elements” (Annex III) which are high-risk AI systems**	
	If full application of hEN, common spec, EU schemes (art. 24.2)	*If not (art 24.2)*	*If full application of hEN, common spec, EU schemes (art. 24.2)*	*If not (art 24.2)*
Presumption of conformity Harmonized standards (art 18.1) Common specifications (art 18.2)	✓	✗	✓	✗
Internal control procedure (based on Module A)	✓ Possible (art.24.2)	✗	✓ Possible[5]	✗
EU-type examination procedure (based on module B) set out in Annex VI followed by ***conformity to EU-type based on internal production control*** (based on module C)	✓ Possible	✓	✓ Possible[4]	✓ Possible[4]
Conformity assessment based on full quality assurance (based on module H)	✓ Possible	✓	✓ Possible[4] Where conformity is carried out under the AI act, the procedure is similar to module H.	✓ Possible[4] Where conformity is carried out under the AI act, the procedure is similar to module H.
(EU) 2019/881 ***EU statement of conformity – Self Assessment*** [Basic CSA art.53] or ***certificate issued by a CAB or NCCA*** [Basic, Substantial and High CSA art.60]	✓ By implementing act to identify eligible CSA scheme to demonstrate conformity (art 18.2) By Implementing act to decide of exemption of CRA third party assessment (Art 18.3)	✗	✓ Possible[4] By implementing act to identify eligible CSA scheme to demonstrate conformity (art 18.2) By Implementing act to decide of exemption of CRA third party assessment (Art 18.3)	✗

Table 2: Type of conformity assessment for products in Class I

[5] Only if the conformity assessment procedure based on internal control referred to in Annex VI of the AI act applies. If the conformity assessment procedure based on Annex VII of AI Act applies, conformity assessment under the CRA does not apply.

Type of conformity assessment	**Class II** **“Critical product with digital elements”** **(Annex III) which are not high-risk AI systems**	**Class II “Critical product with digital elements” (Annex III) which are high-risk AI systems**
Presumption of conformity Harmonized standards (art 18.1) Common specifications (art 18.2)	✗	✗
Internal control procedure (based on Module A)	✗	✗
EU-type examination procedure (based on module B) set out in Annex VI followed by ***conformity to EU-type based on internal production control*** (based on module C)	✓ (art. 24.3)	✓ (art. 24.3) Possible[4]
Conformity assessment based on full quality assurance (based on module H)	✓ (art. 24.3)	✓ (art. 24.3) Possible[4] Where conformity is carried out under the AI act, the procedure is similar to module H.
(EU) 2019/881 ***EU statement of conformity – Self Assessment*** [Basic CSA art.53] or ***certificate issued by a CAB or NCCA*** [Basic, Substantial and High CSA art.60]	✓ By implementing act to identify eligible CSA scheme to demonstrate conformity (art 18.2) By Implementing act to decide of exemption of CRA third party assessment (Art 18.3)	✓ Possible[4]

Table 3: Type of conformity assessment for products in Class II

Type of conformity assessment	**Highly critical product with digital elements** **(Art. 6.5) which are not high-risk AI systems**	**Highly critical product with digital elements** **(Art. 6.5) which are high-risk AI systems** Conformity assessment procedure as defined in AI act art. 43 applies.
Presumption of conformity Harmonized standards (art 18.1) Common specifications (art 18.2)	✗	✗
Internal control procedure (based on Module A)	✗	✓ Where harmonized standards or common specifications have been used, procedure similar to module A.
EU-type examination procedure (based on module B) set out in Annex VI followed by ***conformity to EU-type based on internal production control*** (based on module C)	✗	✗ N/A
Conformity assessment based on full quality assurance (based on module H)	✗	✓ Procedure similar to module H.
(EU) 2019/881 ***EU statement of conformity – Self Assessment*** [Basic CSA art.53] or ***certificate issued by a CAB or NCCA*** [Basic, Substantial and High CSA art.60]	✓ European cybersecurity certificate (Art 6.5)	✗ N/A

Table 4: Type of conformity assessment for Highly Critical products

Eurosmart wants to bring to the attention of the commission the current state of affairs in this regard being the lack of schemes available after two years of implementation of the CRA, the slow progress in this area, and that from the two available candidate schemes available today, only the EUCC is applicable for products with digital elements. Additionally, while EUCC is suitable for Highly Critical products, the market lacks alternatives suitable for Critical Products in domains like IoT and Industrial IoT. A potential IoT scheme developed using input from the essential requirements of parts thereof as set out in Annex I would be the desired development.

3. Highly critical products

As per Article 6.5 from the CRA proposal, the Commission is empowered to adopt delegated acts specifying categories of highly critical products required to obtain a cybersecurity certificate and under which specific European cybersecurity certification schemes (the Member States may also require such schemes). However, the current text doesn't specify what products are considered highly critical products and the required cybersecurity certification. In the context of 6.5(b), it leaves additional ambiguity because while NIS2 could establish the level of security certification required for certain product types, this is not clear when a product is categorized as highly critical due to the "relevant for the resilience of the overall supply chain of products with digital elements against disruptive events". This can create potential conflicts when a product certified at level "Basic" under the CSA could claim CRA conformance.

Eurosmart recommends the commission to activate a delegated act for applicability of NISD2 certification as proof of conformance for highly critical products at the time of the CRA activation, to prevent products from facing a double obligation of certification (from NIS and CRA), as soon as CRA is implemented.

Under Article 6.5, the commission may require certification schemes for highly critical products with functionalities laid down in art. 6.2, that is either

- Used by critical entities under the NIS
- Or relevant for the resilience of the overall supply chair

Hence, the approach is not limited to NIS use cases. As per Article 6.5 from the CRA proposal, when determining products with digital elements for which Cybersecurity certification is mandatory (highly critical products) – the European Commission shall take into account the level of cybersecurity risk. The current proposal does not include any clear provision to anticipate this level of cybersecurity. As such it would be extremely difficult to identify the relevant LoA to be achieved through CSA certification schemes. The update of categories of highly critical products should go alongside the identification of applicable schemes and/or mandate to ENISA to develop new schemes according to Article 8 of Regulation (EU) 2019/881 (CSA). In this context, a level of certification "High" according to CSA should be required for highly critical products.

When a highly critical product is identified and there is no appropriate scheme available, it's not clear from the current draft how the conformance is handled. Eurosmart recommends clarifying this scenario considering the lessons learnt during the development of the two candidate schemes under CSA. In particular, considering the time and effort involved in creating and launching new schemes. As well as to confirm if indeed, such schemes would rely on Article 48(2) of Regulation (EU) 2019/881 (CSA).

Moreover, the update of the requirements laid down in Annex I will directly impact the applicable EU schemes and their maintenance. As per the product categorization, groups of experts dealing with scheme maintenance and CSA conformance requirements needs to be established, giving visibility to manufacturers, CABs, and other relevant stakeholders.

As per the product categorization, a group of experts needs to be established, giving visibility to manufacturers to prepare for the potential adoption of such conformance requirements.

4. Open source

Per recital (10) of the CRA proposal, Open sources are out of the scope of the text. This leaves open questions like how to handle the case of a product with digital elements which relies on an open-source component. According to Article 11.7, the burden lies on the manufacturer when in fact, there is necessarily factual that an entity will address on time, the security vulnerabilities of the open source.

What about the accountability and conformance impact relating to cybersecurity issues coming from the open-source components? What is the legal definition of open source?

Eurosmart recommends reviewing the definition of open-source and potential conflicts on its applicability, and the exception in the proposal. This is particularly relevant for the critical or highly critical products heavily relying on open source like for example browsers, Open RAN, etc.

5. Product categorisation

5.1. Annex III

Eurosmart strongly supports the approach taken by the commission by adopting a risk-based model for the categorization of digital elements, Class I, Class II, and Highly Critical. Based on this risk-based principle, Eurosmart wishes to make the following recommendations:

- The existing list might need to be revised using this principle and support from expert ad-hoc groups and ENISA might be required to establish a taxonomy for defining products, reducing friction in implementing the regulation.
- Besides revising the product categorization, it's important to clarify product definitions. The current list is open to interpretation and prompts confusion. For example, general-purpose Micro Controller Units (MCUs): A microcontroller can be considered a self-contained system with a processor, memory, and peripherals and can be used as an embedded system. While some embedded systems are very sophisticated, many have minimal requirements for memory and program length, with no operating system, and low software complexity. Hence the complexity: manufacturers provide to the market products ranging from bare silicon to devices equipped with ready-to-operate software functionality.
- During the process, it's important to establish the applicability in the context of the risk model. For example, a product from Class I might end up as part of a high-risk product in critical infrastructure, and in some cases, such a scenario might be unavoidable. Therefore, proper classification is highly relevant, as well as acknowledging that the risk models for components and end devices are complementary, but not the same.

6. Requirements for products with digital elements

6.1. Essential requirements

Regarding the "**ESSENTIAL CYBERSECURITY REQUIREMENTS**" as listed in Section 1, Annex I of the proposal, Eurosmart recommends:

- Revising the language of the applicability of the essential requirements as proof of conformity to those applicable to the specific product type and category, as a way to acknowledge the vast number of products, and product configurations and its ability to meet in full, or partial, those requirements. The nature of the applicability of those requirements per product type can be further explored when developing harmonized standards.
- In particular to requirements addressed in Annex I, 1. 3(b), 1. 3(c) and 1. 3(e), it's important to prevent overlapping with other vertical legislation, as could be the case of the Digital wallet regarding data protection (GDPR) or protection against unauthorized access; or the Product

Passport requirements from the proposal for Eco-design for Sustainable Products Regulation, as examples of this overlapping. The articulation with other vertical requirements needs to be established when such requirements already exist.

- An “appropriate level of cybersecurity” might require further guidance for professionals in the security domain, supporting understanding when a certain “good” feature is “good enough”. Particularly relevant for products in Class I and Class II.
  - Alignment with the CSA level could guide in this regard.
  - Documenting the guidance during the development of harmonized standards will help developers qualify specific security features.
- On the requirements for products to “be delivered with a secure by default configuration, including the possibility to reset the product to its original state”, Eurosmart recommends revising the language of this proposal as its current form invites roll-back attacks on hardware products. It adds extra complexity for manufacturers to bring a product to a previous state with an older software version, the “original state”. The requirements can be modified as “…the possibility to reset the product to its original configuration settings”.
- The essential cybersecurity requirements from Annex I, 1.3(k) require that, “*where applicable, through automatic updates and the notification of available updates to users* “. It has to be considered that it does not always depend on the product itself, but on the connectivity of the product, which is not under the sole control of the product, but rather the user. Therefore, this statement should be removed.
- Clarification to the requirement from Annex I, 2.3, with regards to “effective and regular test and reviews of the security”.

As per section 2, Annex I:

- Regarding the requirement of “drawing up a software bill of materials”, Eurosmart believes that a software bill of materials is a positive step in enhancing visibility from the software supply chain, but it’s of not much value without context. SBOMs are not static documents. Every new product release of a component must include a new SBOM. SBOM are of the utmost importance and the requirement to have it mandatory is a step forward. It is very useful to identify impacted items where a vulnerability on a component is identified. However, the management of SBOM will be complex:
  - One SBOM for a version of a product should consider evolving over time or even be divided depending on the products that have received patches
  - Is it possible to have a reliable SBOM and good vulnerability management (including patch distribution) without a good configuration management system and development cycle? How is it possible to achieve it when only requiring Module A, B or C (sufficient for Class 0, class I and class II)?
  - Eurosmart recommends considering adopting specific requirements for the configuration management system and development cycle, listing all configuration items for a specific product together with the exact version of each item relevant to a specific version of the complete product. Beyond listing those components as SBOM will do, it’s more important to understand the role they play in the configuration of the product.
- As per Annex I, 2.1, the “top-level dependencies of the product” are unclear and should be clarified.
- The language on the requirement “remediate vulnerabilities without delay” from Annex I, 2.2, doesn’t reflect the nature of the business, nor provides enough context for the response time. A minimum time is needed to address and remediate a vulnerability which may take days or weeks. Eurosmart recommends amending this requirement to instead require the manufacturer to “commit to the best effort to address and remediate vulnerabilities without

delay". This so-called "best effort" is documented as part of the technical documentation as indicated by Annex V,2.b.

- On 2.3, what is the meaning of effective and regular tests and reviews of security?
- On 2.4 the disclosure of the vulnerability can't take place as soon as the security update has been made available, as it may take time to have it applied on products, especially when the latter are not always connected, and the connectivity depends on the user (e.g., smartcard). It may even happen that not some products on the field may never be patched, despite they are used. Besides, the obligation to communicate the vulnerability that has been patched is also questionable. In some cases, if the vulnerability is critical, it may even be better not to communicate at all and take corrective actions (replacement). All this is already part of the best practices from domains in security.
- On 2.7, the wording "distribute" seems not suitable here as the manufacturer may not directly sell to the final customers (e.g., secure element, software libraries, etc.) but to another manufacturer that crafts the final product. In that case, the distribution of updates also depends on the second manufacturer that shall also accept to put in place the technical means necessary for the secure distribution of the update. Therefore, the wording "make available" should be used instead. Another possibility is to specify that this requirement only applies to the manufacturer delivering the final product to the customer.
- Additionally, to 2.7, it's important to point out that the requirement for a" timely manner" does not only depend on the manufacturer but also on the user itself as it requires that the product is connected which only depends on the user. The wording "timely manner" should therefore be removed.

6.2. Obligations of manufacturers: risk assessment

The Risk Assessment as part of the technical documentation that the manufacturer shall include, according to Articles 10.2 and 10.3 of the proposal when placing a product with digital elements on the market, is to be performed by the manufacturer mainly taking into account the intended use/environment of the product.

In a digitally mature environment, at the inception phase of the product, a risk analysis is performed. Out of this exercise, countermeasures are introduced next to any other product feature that the engineering team has to develop. As product development evolves, those countermeasures are verified at different points, as any other product feature. This approach results in cyber resilience products.

The reality is that product features from developers without enough digital maturity perform functionality dictated by users, market requirements, competitors, prices, and more but definitively they are not the product of a risk analysis.

The CRA initiative presents a unique opportunity to enhance the digital maturity of product manufacturers. However, this is a lengthy process, and we must prevent additional cyber risks arising from the self-assessments of parties without enough digital maturity. It generates exposure for manufacturers while eroding the value of the CRA since by lacking guidance, inexperienced developers working on risk assessment, will result in free-format and open-to-interpretation assessments. This is critical for Class 0 products.

For Class I, even for third-party assessment, there might be a lack of alignment on the definition and applicability of risk assessments. It will be complex ESOs to develop harmonized standards with the risk assessment embedded in the development of such standards given a large number of product types: Password managers, network interfaces, firewalls, microcontrollers, etc.

For that reason, Eurosmart recommends that guidance is provided for risk assessments, supporting all those parties who are new to security and security assessments.

There are existing standard assessment methodologies (e.g. EBIOS[6]) that can be presented in the form of templates, and together with education, will provide a good base for self-assessments. Such guidance could come from ESOs, ENISA, or expert ad-hoc groups to which the experts from Eurosmart will be willing to contribute.

7. Vulnerability management

7.1. Know exploited vulnerabilities

As expressed in Article 10.1 of the proposal, when placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed, and produced following the essential requirements set out in Section 1 of Annex I. Among other requirements, the Products with digital elements shall be delivered without any “known exploitable vulnerabilities”. Eurosmart recommends that the commission further refine this requirement, considering the nature of “knowledge”. When possible, create guidance through ENISA, ESOs, or ad-hoc expert groups, to public sources that manufacturers can consult. This can be resolved by pointing to the future ENISA European vulnerability database where publicly known vulnerabilities will be listed.

Moreover, it’s important to create awareness that even in the event of identifying exploitable vulnerabilities, they don’t translate into immediate risk, and yet, when they are made public, it’s when the real risk gets introduced. Other factors like the likelihood of the event, the complexity of the attack, and even market adoption play a role in considering the exploitation of such vulnerabilities.

Once the product is on the market and vulnerability is identified, the provision “shall be delivered without any known exploitable vulnerabilities” will stop any commercial activity. This will be especially harmful to hardware products in different Classes, and all the players in the value and supply chain will be impacted. Eurosmart recommends a hybrid approach for products with remote update capabilities. This technical capability with a vulnerability handling process as required by Annex II will enable manufacturers to handle vulnerabilities on the field at all the different stages within the value chain: from manufacturing, reselling, deployment, commission, decommission, etc.

Eurosmart recommends clarifying the scope and applicability of provisions under:

- Annex I 1.2 referenced in article 10.1 (obligation for manufacturers): “Products with digital elements shall be delivered without any known exploitable vulnerabilities”.
  - A definition of “exploitable” vulnerability should be added in article 3, considering the meaning of an “exploitable” vulnerability in the context of (1) the foreseen usage and (2) the risk assessment. It shall be noted that a product may be used in a different context, and within each context, the meaning of exploitable vulnerability – thus the skills and capacity of attackers – may differ.
  - During the risk assessment as defined in article 10, the consideration of (1) exploitable vulnerability, and (2) quantification of risks/expertise of attackers should be added. These aspects should also be reflected in Annex I 1.2.
- According to Annex I 2.2 referenced in article 10.1 (obligation for manufacturers): “[…] concerning the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates”
  - It should apply to exploitable vulnerabilities only.

[6] https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/

- Article 10.6 reads "Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Section 2, point (5), of Annex I, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources"
    - Only exploitable vulnerabilities should be processed and remediated.

The wording "level of cybersecurity risk" as introduced in the text is unclear and should be defined in article 3. Besides, this level should be assessed on a case-by-case basis following the risk assessment to specify its meaning in terms of (1) exploitable vulnerability, and (2) quantification of risks/expertise of attackers.

7.2. Vulnerability reporting

The complete CRA requirements should apply 24 months after the entry into force of the regulation, except the reporting obligations on **actively exploited vulnerabilities and incidents for products on the field,** which would apply **12 months** after the entry into force of the regulation for all the product on the field or put on the market. For one year, manufacturers will be obliged to report "actively exploited vulnerability" without any obligation of risk assessment/risk management processes. This creates an ambiguity as it can be translated as manufacturers should assess the meaning of an exploitable vulnerability when a risk assessment hasn't been carried out. Eurosmart recommends clarifying this scenario.

7.3. Vulnerability handling

Since the CRA could potentially rely on CSA schemes as the presumption of conformance mechanism, Eurosmart recommends that CRA vulnerability handling is aligned to the current methods and policies developed under the CSA to prevent misalignment in the interpretation and implementation of this requirement.

7.4. Mechanisms and supervision for the reporting of vulnerabilities and issues

As pointed out in the "**Interplay with existing policy provisions in the policy area**" section, other vertical legislations have already defined and set up mechanisms and supervision for the reporting of vulnerabilities and issues:

- eIDAS for security breach for Trust services, …
- GDPR for data breach;
- AI Act for reporting serious incidents and malfunctioning AI systems;
- …

The CRA also introduces its mechanisms and supervision for the reporting of vulnerabilities and issues. It is likely to bring substantial complexity to stakeholders, including supervision authorities. Eurosmart recommends simplifying it.

8. Conformity assessment

8.1. Conformity assessment procedures for products with digital elements

8.1.1. Interoperability of Articles 18 and 24

There seems to be a contradiction regarding conformity assessment requirements for highly critical products:

- Article 6.5 states: “The Commission is empowered to adopt delegated acts per Article 50 to supplement this Regulation by specifying categories of highly critical products with digital elements for which the manufacturers shall be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme according to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof”.
    - While to particular level is indicated, it seems reasonable to consider that a level of certification at least “Substantial” is required given the nature of the risk for this product type.
- Article 18.3 defines the presumption of conformity as: “Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 and specified as per paragraph 4, shall be presumed to conform with the essential requirements set out in Annex I in so far as the EU statement of conformity or cybersecurity certificate, or parts thereof, cover those requirements.
    - This opens the possibility that a simple statement of conformity (e.g. level “Basic”) will be accepted for a highly critical product (which is a product with digital elements) under CRA.
- Article 6.5 first sentence regarding highly critical product seem unclear: “The Commission is empowered to adopt delegated acts per Article 50 to supplement this Regulation by specifying categories of highly critical products with digital elements for which the manufacturers shall be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme under Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof”
    - Does it mean that the commission is empowered to specify categories of highly critical products with digital elements and may optionally also specify the European cybersecurity certificate under a European cybersecurity certification scheme according to Regulation (EU) 2019/881 to obtain to demonstrate conformity?
    - Does it mean that the commission is empowered to specify categories of highly critical products with digital elements and the mandatory European cybersecurity certificate under a European cybersecurity certification scheme under Regulation (EU) 2019/881 to demonstrate conformity?
- The way to demonstrate conformity for class II critical product seems ambiguous:
    - Under Article 18.3, an EU statement of conformity or certificate which has been issued under a European cybersecurity certification scheme adopted as per Regulation (EU) 2019/881 could be used to demonstrate the presumption of conformity of a product with digital elements (which includes class II critical product).
    - Under article 24.3, class II critical products conformity shall be assessed either by using module B + C or module H. EU statement of conformity or certificate which has been issued under a European cybersecurity certification scheme adopted as per

    - Regulation (EU) 2019/881 can't be used, while they are allowed for class I critical products (refer to article 24.2
- The way to demonstrate conformity for class I critical product seems unclear
    - Article 24.2 talks about "European cybersecurity certification schemes" without providing a definition or interpretation of equivalence to basic, substantial or high levels.

Eurosmart recommends the commission address those definitions that can help for a better interpretation of the requirements and their applicability for demonstrating conformance.

8.1.2. Harmonized standards

Where harmonized standards do not exist or are insufficient or where there are undue delays in the standardization procedure or where the request by the Commission has not been accepted by the European standardization organizations, the Commission may, by the means of implementing acts, adopt common specifications.

The use of harmonized standards should be privileged over common specifications. The objective of a harmonized standard is:

- ensuring consistency with the requirement of given legislation and,
- promoting interoperability among the developers.

If the Commission relies on "common specifications", the latter won't be achieved. In addition, the risk is that adopting common specifications generates too much complexity for placing products in the market without clear cybersecurity added value. Standardization requests to the ESOs must be the baseline scenario, all these standardization requests must be accompanied by a request to develop risk assessments according to the vertical or product category.

However, the common specification should not be discarded as they may appear to be very useful to demonstrate the conformity of legacy products for which a whole framework of conformity assessment material already exists (for example banking cards). Therefore, the common specification shall not be considered as an alternative to harmonized standards, but rather a complementary approach (Article 19). Indeed, it shall only be possible to reference conformity assessment materials (1) provided it is demonstrated that it ensures fulfilment of (some of) the requirements of Annex I and (2), to support a smooth transition. Besides, under the current text, it can only be used for Class I products. It should also be made possible for Class 0 and Class II products so that existing legacy conformity assessment materials could be reused, provided it ensures the fulfilment of essential requirements described in Annex I.

The functionality of the product, intended use and extent of impact should be considered in the creation of the harmonized standards: merging device components and end devices in a single category, produce an additional burden for the whole ecosystem. End devices gain security capabilities from the components, therefore requiring different types of assessments.

The High-Level Forum should involve the identification and priorities in terms of harmonized standards to support the CRA requirements. This group will facilitate the identification of the standardization activities of strategic importance for the EU and will facilitate political concertation between the Commission and the Member States on such priorities.

8.1.3. 3rd party assessments for Class I and Class II products

Eurosmart welcomes the proposal in the CRA of the selection of the conformity assessment procedures based on Module A, Modules B plus C, and Module H, following a risk-based approach. In that regard, and specific to the 3rd party assessment procedures, Eurosmart wants to call the attention of the commission that some of the digital elements listed in Annex III, and others not listed yet but potentially falling in Class I or Class II, are being assessed and certified by private institutions, or in the process of implementing security certification schemes for those products. Examples of those organizations and schemes are GSMA, EMVCo, PCI, CSA (Connectivity Standards Alliance), Common Criteria (ISO/IEC 15408, ISO/IEC 18045), GlobalPlatform SESIP, PSA Certified, etc.

For this reason, Eurosmart recommends, to prevent work overhead from performing 3rd party assessment of products with digital elements the commission, in collaboration with ENISA, ESO, and ad-hoc expert groups, considers the potential applicability and reusability of private 3rd party private schemes. There are industry standards available today that with the proper mapping, can serve as evidence of conformance for products under Class I and II. It's important to acknowledge that implementing the CRA without any consideration to the existing security assessments adopted in the industry as best practices, many of them in alignment with the CRA proposal from Annex I will result in additional burden and cost for manufacturers and consumers alike.

An additional benefit of this approach comes from acknowledging there are no harmonized standards, nor enough expertise in cybersecurity at ESOs, Notify Bodies, ENISA, and other private institutions for addressing type approvals of a large catalogue of product types. Plus, experience has proved that it can take more than a year to create one set of harmonized requirements per product category. The same applies to the creation of schemes under the Cyber Security Act.

A mechanism should be introduced in Article 18 to formally engage and consult stakeholders in the definition of procedure for the presumption of conformity. This is needed as many things (procedures, tests, methodologies) have already been put in place in various sectors, and they should be allowed to have their say to make sure that what is in place is properly reused and recognized as means to presume conformity. In that regard, Eurosmart suggests creating an expert group gathering stakeholders for that purpose.

8.2. Need for modularity and reusability in conformity assessments

8.2.1. Modularity and reusability

It is of particular importance for manufacturers to ensure that their products do not contain vulnerable components developed by third parties: The cybersecurity of the entire supply chain is ensured only if all its components are cyber-secure. This principle is laid down under Article 10.4 as due diligence obligation for manufacturers and reflected in the product examples listed in Annex I, Class I, and Class II.

However, introducing mandatory security requirements in a wide range of devices placed in the EU's 'single-market place' poses challenges for device manufacturers, especially small and medium-sized enterprises.

- They face challenges to integrate security features in their Products due to limited security know-how and testing resources.
    - End device developers are not security specialists, their focus and skills are specialized in other areas.

    - There are not enough security specialists in the market[7] and acquiring capability is more effective than developing it, with the intrinsic business benefits of bringing products on-time to market.
- Developers should show compliance to build adequate trust in their products for consumers as well as regulators (market surveillance).
    - At the time of a security assessment, they will be challenged to address questions concerning security functionality provided by 3rd party components suppliers.
    - Getting access to that information might not be easy for several technical, legal, contractual, or other business reasons.
    - Besides, this approach is not scalable when the supplier of those components has to support each device developer individually.
- Device Manufactures have to stay price competitive despite additional security features.

Those are some of the reasons why products with digital elements rely on the core security capability provided by the components embedded into their products, covering hardware and software components providing core security functionality.

There are mechanisms enabling device developers to reuse the evidence of the capabilities on their devices for showing conformance to security device requirements when such security capability is properly integrated. This approach to security is called composition. Security evaluation schemes like Common Criteria (ISO/IEC 15408 and ISO/IEC 18045) and SESIP work using those concepts.

It is key to address the challenges of device manufacturers and their ability to show conformance to CRA, to consider the:

- Encapsulate the security functions in discrete secure element components or a 'security sub-systems'.
    - For example, define a security target in a digital device that should fulfil the CRA security functional requirements.
    - A digital device could have multiple such security components fulfilling the essential requirements.
- Allow composite evaluation methods.
    - Security critical components e.g. password managers, firewalls, and Microcontrollers should require 3rd party testing while the device makers that use 'such certified' components thereby can do self-assessment to declare conformity.
    - When the manufacturer uses third-party assessments, the assessment party can focus on the proper integration of the secure pre-certified components rather than testing the security functionality of the device, resulting in time and cost-effective, scalable assessments.
    - This requires an evaluation method that allows for composition such as Common Criteria, SESIP, etc.

Eurosmart recommends the commission consider adopting a similar model of smart composition for CRA conformance assessments as this delivers several benefits for suppliers of components, developers of devices, and assessment bodies. It enables them to (1) better control the security as the core of products with secure elements in a scalable manner, (2) reduce cost, and (3) decrease the time to market which is instrumental to serving the market with products. These elements are key for a successful CRA implementation.

[7] (ISC)² Cybersecurity Workforce Study 2022
https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

This requires acknowledging under the CRA proposal:

- In the same way that components sourced from third parties in products with digital elements could introduce vulnerabilities compromising the security of the products, consider that when a manufacturer of end devices makes use of secure, certified, or in conformance components with the essential requirements, it enhances the security assurance of the end devices, reducing effort on the assessments.
- Proposed methodology assessments (especially for software), standards and related risk assessments should reflect this possibility and whenever possible and applicable, incentivize this approach.
- Certification of end devices and components should reflect this practicality as the focus, functionality, and risk are different among them.
- Finally, considerations need to be taken in this regard, as there is an intrinsic need for transition periods in the entire stack: The IoT products built in 2026, 27 and 28 are based on the components designed TODAY and who might need to be first showing conformance with CRA.

8.2.2. A CE mark of CE marks

As per Annex III, core sub-components of end devices are in the scope of the CRA applicability. Each of them as an individual product will need to demonstrate conformance with the essential requirements and eventually obtain its own, individual CE mark.

Considering for example a product like a mobile consumer device (MCD). This product is composed of:

- An operating system.
- The main system-on-chip (SoC) module is supported by secure crypto processors.
- A few general-purpose microcontrollers (MCU) and application-specific integrated circuits (ASIC) control memory, power, interfaces, etc.
- At least one hypervisor supporting virtualized execution of operating systems
- At least one secure element

As the conformance assessment of the MCD is performed, the large number of security capabilities on the device itself will be provided by those individual components and the CE mark of the MCD will be largely the sum of the individual CE marks from sub-components, when properly integrated.

Moreover, the manufacturer might have product lines of MCDs from different materials and dimensions, models, and yet, the core security capability is the same across all of them.

This is an example of how the relevance of adopting a modular approach, and composition as a tool for assessment, is relevant in the context of CRA to have a scalable implementation. It’s for that reason that Eurosmart recommends the commission consider acknowledging composition and modularity as part of the CRA.

8.3. Notified bodies

8.3.1. Conformity assessment bodies', notification and assessment

Eurosmart calls on strengthening the provisions of Chapter IV when it comes to the specific requirements applicable in the security domain. Notification and assessment should be independently conducted whether the third-party assessment comes from a public or private institution.

Moreover, the requirements related to the notification of CABs (art 29) as such, could lead to several interpretations. Article 30 specifies that the presumption of conformity to these requirements could be reached through harmonized standards published in the Official Journal of the European Union. To avoid any future misalignment Eurosmart recommends relying on and referring to standards ISO/IEC 17065 and ISO/IEC 17025 as is already the case in the Cyber Security Act for CABs performing assessments in the security domain.

8.3.2. Update of the "blue guide" and inclusion of applicable "explicit" requirements for Notified Bodies

Article 29 lays down generic requirements for Notified bodies. These elements are not explicit enough to ensure a concrete implementation of the assessment and the supervision of Notified Bodies. The guidance provided by the Blue Guide is, therefore, necessary to ensure consistency amongst national authorities and notified bodies. To provide legal certainty these "concrete" requirements should be linked with the CRA and legally binding, for instance, the legislator could refer to the blue guide in article 29 or specify the implementation of this requirement through implementing acts.

The ISO/IEC 17065 for the certification party, and the ISO/IEC 17025 for the evaluation party, must be in the security domain, and not to assume that safety accreditations are in the same domain or they can be used in consequence for security assessments. This must be reflected as well in a future revision version of the "Blue Guide" on the implementation of EU product rules 2022 (2022/C 247/01). Although understandable as an evolution of a document largely focuses on safety, it's very important to frame the security aspect of the expertise from third-party assessments. This will prevent misalignment on the applicability of the regulation due to the lack of security professionals on the assessment parties, experience from Notify Bodies in the domain, and insufficient guidance.

The CRA intends to provide a transparent accreditation process for Conformity Assessment Bodies (CABs) to enhance the level of confidence in certificates of conformity anywhere in the European Union. However, the Member States designated a notifying body responsible for CAB accreditation may decide not to rely on Regulation (EC) No 765/2008, which is the common basis for CAB accreditation in many other pieces of EU legislation (Recital 49 and Article 26). This approach will lead to serious discrepancies a) amongst the accreditation and assessment process chosen by the Member States made b) with several EU legislations which cover products falling under the scope of the CRA. For instance, (EC) No 765/2008 is the base ground for CABs evaluation through the New Legislative Framework, the Cybersecurity Act EU CSA (2019/881) and the Artificial Intelligence act.

Moreover, the requirements related to notified bodies (Article 29) as such, could lead to several interpretations. Article 30 specified that the presumption of conformity to these requirements could be reached through harmonised standards published in the Official Journal of the European Union. To avoid any future misalignment Eurosmart recommends relying upon and referring to the standards ISO17065 and ISO 17025 as is already the case in the Cyber Security Act.

Lastly, the CRA does not provide any peer-review mechanism. This approach has been adopted for the Cyber Security Act. Eurosmart encourages the legislator to consider this approach to ensure better consistency between the two pieces of legislation and, at the same time, to increase the level of trust among the Member States.

8.3.3. Necessary consideration for performing CRA evaluation on European territory

Third-party assessment could imply access to the source code of a product with digital elements. The relationship between the developers, manufacturers and the CABs is based on trust and formalised by a Non-Disclosure Agreement (NDAs). An evaluation performed outside the EU territory could be a risk for the industry when it comes to their IP, trade secret, and choice of jurisdiction, as well as the impact on the extra-territoriality of non-EU countries. This aspect is essential for the strengthening of European digital sovereignty. In this respect Article 29 provide that Notified bodies should be granted a legal personality under an EU national law. This approach is not bringing enough safeguards and Eurosmart recommends legislators consider the evaluation process to be carried out in the EU territory. Besides, it must make sure that the extraterritoriality of non-EU countries' laws is not impacting these activities.

This approach is particularly relevant when a notified body subcontracts or has recourse to a subsidiary. The provisions of Article 31 could be an opportunity for notified bodies to act as “empty shells” and to perform their activities outside the European Union to offer better prices. Eurosmart calls on the legislator to provide additional safeguards, narrowing this option to very specific tasks.

8.3.4. Additional clarifications

- The interoperability of Articles 26.2 and 32.2 regarding the use of the national accreditation body to have CAB notified (to be a notified body) is perceived as a contradiction and it requires clarification.
- The text from Article 44.3 seems to refer to article 11 of regulation 1025/2012 instead of article 10.
- The commission should consider that given the nature of the information, Article 52.2shall require the agreement from the manufacturer and/or importer and/or distributor of the product at stake.
- Article 53.3 should be revised in the applicability of penalties, as they should also apply in case of non-compliance with provisions of Article 13 (for importers) and Article 14 (for distributors).

9. CE marking & cybersecurity labelling

9.1. The CE Mark

In contrast to the European cybersecurity certification framework under CSA that will centralise all the information related to certified products to inform the end-users; the current conformity assessment procedures are not designed to deliver information on security functionalities to the end users, but rather a guide. In that sense, there won’t be a single repository point where the consumer can verify the security, and Class of the product in use beyond the CE mark that implies compliance with CRA requirements. The preliminary impact assessment issued by the Commission in 2022, included the possibility to define a communication label, such a proposal is no longer reflected in the current text.

The implementation of any mark for identifying the security capabilities of a device, or to be used based to support the claim that the product is secure, or cyber resilient, it's a topic largely studied in the industry. Examples are the report by Mozilla Open IoT Studio[8], the Singapore standard for Cybersecurity labelling for consumer IoT[9], and the ISO/IEC NP 27404[10]. In summary, the use of the label or mark for cybersecurity should inform consumers while preventing misleading assumptions about what it means "secure". Other domains have adopted an approach on the label reflecting the levels of service, relevant to the user and use case as a way to inform and educate the market, as is the case of the energy efficiency labels.

It's for the above reason that Eurosmart recommends the commission prevent the multipurpose of the CE mark drive the message of cyber security capabilities on products with digital elements by itself. This needs to be complemented with "real-time" information as per the status of vulnerabilities, (assurance) Class, and evidence in the form of assessments or certification that the product has been summited for the type approval. This should be accessible, visible and reachable to users. This will inform them, allowing them to make informed decisions.

A similar approach has been adopted under the Cyber Security Act, Article 54,1(i) of Regulation (EU) 2019/881, with ENISA developing a label, in conjunction with a repository, where consumers will be able to get additional information about the product security capabilities and robustness of such capabilities. Eurosmart recommends following this approach and coordinating this effort with ENISA to prevent fragmentation of the information in the market.

To ensure the right level of information, Eurosmart recommends relying on the current EU-CSA labelling proposal. This label is bound with the deliverance of an EU cybersecurity certificate or an EU 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.

By extension and in addition to the CE marking, this label could be used to show the conformance of products with digital elements to the CRA. For instance, the provisions of Annex II could be provided to the end-users through a seal referring to a common database managed by an independent authority and maintaining the information up to date.

[8] "A Trustmark for IoT", Peter Bihr, Mozilla Open IoT Studio, 2018
https://thingscon.org/publications/report-a-trustmark-for-iot/

[9] "Cybersecurity labelling for consumer IoT", TR 91:2021, 2021
https://www.singaporestandardseshop.sg/Product/SSPdtDetail/41f0e637-22d6-4d05-9de3-c92a53341fe5

[10] "Cybersecurity — IoT security and privacy — Universal cybersecurity labelling framework for consumer IoT", ISO/IEC NP 27404, November 2022
https://genorma.com/en/project/show/iso:proj:80138

10. Market surveillance and enforcement

10.1. Product and security maintenance

During the life of a product, changes can occur as the industry adopts Agile development methodologies where products are placed in the market and continuously enhanced with new services for the benefit of users. This is particularly applicable in the area of connected (end) devices or IoT. Some of those changes might not have any impact on the security of the product and account for simply regular functionality while others, due to architectural designs or the constrained nature of the device, while not security relevant could impact the security services in the product. There are changes security specific as a patch management mechanism in response to newly discovered vulnerabilities.

Eurosmart recommends the future dedicated administrative cooperation group (ADCO) consider those scenarios when it comes to product maintenance, with a vision to distinguish between the traditional market surveillance from a safety perspective, and the nature of security, as security is not static.

10.2. Impact of CSA schemes surveillance in the context of CRA conformance

Eurosmart recommends the commission provide guidance documentation on the applicability of the market surveillance when the products show conformance with CRA through evidence from CSA schemes, as under each of those schemes, specific certificate surveillance mechanisms are in place. Those CSA scheme surveillance mechanisms have been designed using the elements described in the previous paragraph.

10.3. Highly Critical products and their maintenance

The CRA proposal establishes a conformance model and its applicability via delegated acts. However, the market surveillance aspect doesn't refer to that kind of product. Eurosmart suggests providence as this has implications regarding the NIS2 implementation, its requirements, and the CSA as per the paragraph above.

10.4. Product withdrawn

Article 10.12 indicates that products may be withdrawn or recalled by the manufacturer during a given period of up to 5 years. Article 43.1 allows market surveillance authority to require the economic operator to take any appropriate actions including withdrawing or recalling the product at any time, making it seem in contradiction with 10.12. Eurosmart recommends adding a clarification to this apparent misalignment.

Additionally, there are discrepancies regarding the period during which products may be recalled when the entity knows or have reason to believe that the product is not in conformity with the essential requirements of Annex I

- **Article 10.12 – manufacturer**
  - "From the placing on the market and for the expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer is not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to

recall the product, as appropriate."

- **Article 13.6 – importers**
    - "Importers who know or have reason to believe that a product with digital elements, which they have placed on the market, or the processes put in place by its manufacturer, is not in conformity with the essential requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity with the essential requirements set out in Annex I or to withdraw or recall the product, if appropriate."

- **Article 14.4 – distributors**
    - "Distributors who know or have reason to believe that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with the essential requirements set out in Annex I shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity are taken, or to withdraw or recall the product, if appropriate."

Eurosmart recommends that Articles 13.6 and 14.4 shall be aligned with the provision of article 10.12.

11. Closing comments

11.1. Resources allocation

Taking into consideration the effort involved in the further development, implementation, and execution of the proposal, framing it in the context of the experience of developments like the Cyber Security Act and NIS2 implementation, the creation of RED harmonized standards, existing security capabilities at national levels and notified bodies, and the future regulatory compliance stack in cybersecurity, Eurosmart recommends the commission revising the resources allocation at ENISA and DG CNET. The current proposal utilizing 4.5 FTEs from the existing ENISA resources, and 7 additional resources under DG CNET sounds quite conservative and comes across as a potential risk for the CRA developments.

11.2. Delegated Acts

The CRA proposal makes use of extensive use of Delegated Acts. All technical details regarding the text implementation are deferred to them, creating a lack of visibility for stakeholders.

Eurosmart recommends clarifying as much in advance as this will reduce market uncertainty and support the proposed act's successful implementation.

11.3. Eurosmart in support of the CRA proposal

Eurosmart celebrates the commission's intention to collaborate internationally to build cybersecurity resilience capabilities by collaborating with international institutions and governments outside Europe. Fragmentation is a natural inhibitor for adoption, and inaction is not an option when we want to address the fundamental problems behind cyber incidents. Building Mutual Recognition Agreements (MRAs) for showing conformance to cybersecurity essential requirements as has been done in other areas will reduce the fragmentation and support the industry adoption worldwide.

Eurosmart welcomes this step forward. The Cyber Resilience Act proposal’s (CRA) requirements should be considered as a common, risk-based, and transversal basis to address cybersecurity. Depending on the intended use and/or the environment, these requirements should be translated into suitable standards and evaluation methodology. Moreover, already adopted tools, such as cybersecurity certification under the European Cybersecurity Certification Framework, could provide the same effects. A large part of the cybersecurity ecosystem is supportive of cybersecurity certification as a way to demonstrate conformance and manage information and business risk. The cybersecurity certification remains the only guarantee to provide a certain level of robustness, guarantee that solutions and products are backdoor-free, and maintain them at the “state-of-the-art”. Eurosmart invites the legislator to make sure that CRA’s approach remains complementary to cybersecurity certification. For instance, CRA’s requirements should be fully compliant with EU CSA’s schemes; and what is more, support the development and use of EU cybersecurity schemes to demonstrate market compliance.

About Eurosmart

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com

@Eurosmart_EU

@Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com