EUROSMART
The Voice of the Digital Security Industry

Cyber Resilience Act

Eurosmart's feedback on ITRE and IMCO amendments

Eurosmart welcomes the recent ITRE draft report and IMCO draft opinion on the Cyber Resilience Act (CRA) and in particular the work achieved by MEPs Nicolas Danti and Morten Løkkegaard to provide more consistency with the already existing EU cybersecurity regulatory landscape.

As an organization dedicated to promoting secure digital interactions and privacy protection for individuals, Eurosmart believes that the consolidation of a comprehensive and harmonized framework for cybersecurity is essential to safeguard the European digital economy and society as a whole. The Cyber Resilience Act is a critical step towards achieving this goal.

Eurosmart believed that the proposal deserves further improvement to adequately integrate suitable cybersecurity evaluation processes. The CRA relies on the NFL (New Legislative Framework) which has been designed for safety purposes only, adaptation of the draft Act provisions and additional links with the EU cybersecurity certification framework under the Cybersecurity Act are therefore necessary.

However, for many market segments, the European hardware security industry already relies on cybersecurity certification schemes and soon on the EUCC scheme. This approach is extremely demanding in terms of security assessment which includes penetration testings for the highest level, vulnerability management and disclosure. The CRA framework relies on modules with a lighter approach that do not highlight security issues at a such level of details. Eurosmart recommends the co-legislators carefully considering the obligations made to the manufacturers that already have their products certified, some CRA obligations in the light of the exigence level requested by CSA schemes would be extremely detrimental for the most advanced European security hardware. From a general approach, Eurosmart supports the efforts of the European Parliament to strengthen cybersecurity in the European Union, and we look forward to further discussions on the Cyber Resilience Act. To build up this coordinated and comprehensive approach to cybersecurity, Eurosmart would like to invite the Members of the European Parliament to consider Eurosmart's comments on significant amendments and in particular the following aspects:

1. Definition of product categories

To provide legal certainty to economic operators and to correctly implement the provision of the CRA the exact definition of the categories of products included in Annex III is necessary. Depending on the definition, some subtype of product may be included or not within Annex III. Moreover, depending on the classification, the assessment approach will vary, products that are already on the field may already be subjected to certain type of certifications whose approach should be adapted to comply with the CRA. With no clear category definition, it would be complex for the economic operator to invest in this anticipation.

The definitions of the product categories should be part of the text alongside the product categories themselves, or the entry into force of the regulation shall be bound to the adoption of these definitions by delegated act. Finally, discussing the content of Annex III without having at hand the corresponding definitions may pervert the discussion of co-legislators on product categories and deprive them from their effective prerogatives.

2. Products lifetime

It is hardly possible to guarantee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development. Multiple examples demonstrate this situation. The expected lifetime should be freely determined by the manufacturer based on its technical capacities. Depending on the technologies, types of products, the risks, and the criticality, the manufacturer may be able to guarantee a more or less long lifetime, which in some cases may be below 5 years.

The right approach is to ensure transparency for consumers. Product lifetime should be clearly indicated in the EU declaration of conformity, which is available to the consumer, so that the latter could make its choice in a fully informed manner.

3. Vulnerability handling and incident reporting

This proposal considers that vulnerability handling can always be ensured over a product lifetime of 5 years which is not at all the case. For some technologies or types of products, it may be challenging for manufacturer to ensure sustainable and long-lasting products as the risks are constantly evolving and increasing. In many situations, while the level of resistance of the product with digital element can be estimated and committed by the manufacturer over a medium period of time (e.g. 3 to 5 years) starting from the development of the product with digital elements, or the placement on the market of the first item, it is hardly possible to guarantee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development.

Moreover, Eurosmart welcomes the proposal to only report significant incidents on a mandatory basis. This approach alleviates the burden for manufacturer and ensures that only relevant and useful information about incidents is notified. The definition of “significant incidents” should be included to provide a legal basis for the manufacturer.

4. Reporting obligations of actively exploited vulnerability

The notification process as amended by the ITRE rapporteur is much more realistic thanks to the proposed notification procedure. This procedure leaves more time for manufacturers to gather information and carry out the needed analysis. Besides, Eurosmart welcomes the need-to-know principle for the disclosure of vulnerabilities which can’t be corrected or mitigated.

When it comes to the applicability of reporting obligation for product with digital elements that have been certified (EUCC EUCS etc.), a deeper analysis would be necessary to align the obligations from the scheme perspective. Finally, efforts to align the provisions with NIS2 are very much appreciated.

Eurosmart suggests addressing vulnerabilities talking into consideration the following aspects:

- Vulnerabilities should only be considered when the product is used in compliancy with the user guidance;
- The assumption of Notification to users should consider the scenario when Manufacturers will often not know who the users are;
- It should be understood that some vulnerabilities cannot be fixed;
- It won't always be possible to disclose information about products when trade secrets are involved;
- The timing of a notification of vulnerabilities should start once the manufacturer has confirmed that it is indeed a vulnerability;
- The period of mandatory maintenance could lead to additional costs within the supply chain.

5. Expert group

The proposal to establish an expert group is an instrumental to ensure the correct implementation of the CRA. Moreover, as cybersecurity is a matter of moving target, it is expected to continuously update and enhance the applicable standards, methodologies, as well as the conformity assessment procedures in a broad sense with the essential requirements. From this perspective the holistic view from experts representing different industry verticals, conformity assessment bodies, standardisation organisations and public bodies active in the field, is a paramount objective.

Eurosmart recommends the co-legislators to carefully consider the composition of this group, the European Standardisation Organisations and National authorities (National Bodies) should be represented within this group. The CRA does not apply to products exclusively developed for military and national security purposes, therefore Europol and European Defence Agency participation is not relevant Moreover, the composition of the private stakeholders' membership should ensure the representativity of many verticals, which could be ensured by business organisations. Finally, as the CRA will rely on EU CSA certification, stakeholders providing technical inputs to ensure the maintenance of the schemes should also be involved.

Moreover, some missions of the expert group conflict with the advisory or divisionary functions of other EU's technical groups. For instance, the certification of highly critical products is mandatory and should not be discussed. However, the group should advice on the type of products falling under this category. Moreover, when it comes to relying on certification, the maintenance of the scheme and the necessary Protection Profiles should be addressed per vertical. For these topics, ENISA, ECCG representatives and future maintenance organisation representatives are relevant.

6. On standards and harmonised standards availability

The proposal acknowledges that when possible harmonised standards should be the privileged approach. Harmonised standards confer a presumption that products to be made available on the market are in conformity with the essential requirements laid down in the relevant Union harmonised legislation. However, as the CRA embrace a wide range of verticals, it seems reasonable to make the

best use of the industrial and technical legacy in terms of “industry standards / industry common specifications” which could be easily translated into “common specifications”.

Finally, taking into account the huge standardisation effort requested by the proposal, when possible, the standardisation toolbox should not be limited to harmonised standards. Eurosmart recommends making the best use of available European Standards and European standardisation deliverables (harmonised standards, European standards and Technical specifications) as defined in Regulation (EU) 2022/2480.

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Exclusion of spare parts	ITRE	2(4)(a)	40	***This Regulation does not apply to components that are exclusively manufactured as spare parts for other products with digital elements that have been placed on the market before ... [40 months after the date of entry into force of this Regulation].***	Positive		Provide a definition for spare parts
Exclusion of spare parts	ITRE	2(4)(a)	213	***4a. This regulation does not apply to spare parts that are exclusively manufactured in order to repair products with digital elements that have been placed on the market before the application date of this regulation referred to in Article 57.***	Positive		
Substantial modification	ITRE	3(1)31	237	'substantial modification' means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed, ***excluding security and maintenances updates that aim to mitigate vulnerabilities***	Positive		Keep this proposal
Incident	ITRE	3(1)(39a)	44	***'incident' means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;***	Positive	Provide definition for incident in line with NIS2	
Definition of product categories	ITRE	6(1)	256	Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. ***Only*** products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as falling into that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the	Positive	This proposal clarifies the rules to apply in case of composition of a component in a product with digital elements	Keep this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				level of cybersecurity risk related to these products. ***The integration of a component of higher class of criticality does not change the level of criticality for the product the component is integrated into.***			
Definition of product categories	ITRE	6(3)	48	The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. The delegated act shall be adopted [by ***6*** months since the entry into force of this Regulation]	Positive with comments	The proposal is an improvement compared to the initial proposal. However, It will be very complicated for economic operators to implement this regulation as the exact definition of the categories of products included in Annex III will come **AFTER** the adoption of the text. This lack of clear definition creates uncertainty for the stakeholders. Depending on the definition, some subtype of product may be included or not within Annex III. The definitions of the product categories should be part of the text alongside the product categories themselves. It is essential for economic operators that have visibility of the product falling within the provisions of Annex III. Discussing the content of Annex III without having at hand the corresponding definitions may pervert the discussion of co-legislators on product categories and deprive them from their effective prerogatives.	Add the definitions of the product categories described in Annex III within the text at stake. Or Enforcement of the Regulation to be conditional on the adoption of these delegated acts
Critical products	ITRE	6(3)	260	The Commission is empowered to adopt a delegated act in accordance with Article 50 to supplement this Regulation by specifying the definitions of the product categories under class I and class II as set out in Annex III. ***If it expands the scope of the product categories, the procedure in paragraph 2 should be followed.*** The delegated act shall be adopted [by 12 months since the entry into force of this Regulation]. ***The Commission shall establish a process under which a product which is a candidate to be***	Positive with comments	The proposal makes sense for future critical products, however Annex III already deserves more specific definition to be fully applied.	Add the definitions of the product categories described in Annex III within the text at stake. Or Enforcement of the Regulation to be conditional on the adoption of these delegated acts

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				a critical product can be reviewed in a collaborative process by all relevant stakeholders, including manufacturers and users, to assess the security risk posed by potential cybersecurity issues with the product, whether and how much designating the product as critical would likely reduce that risk, and the costs associated with designating the product as critical. If such assessment clearly establishes that designating that product as critical would materially reduce the security risk posed to the users of the product and that the value of such reduction would outweigh the costs to the manufacturer and other parties, the product may be designated as critical under this Regulation.			
Critical products	ITRE	6(4)(1a) new	49	***Where a new category of critical products with digital elements is added to the list in Annex III by means of a delegated act pursuant to paragraph 2 of this Article, it shall be subject to the relevant conformity assessment procedures referred to in Article 24(2) and (3) within 12 months of the date of adoption of the related delegated act.***	Positive with comments	Despite the short time frame, this provision brings more visibility to economic operators so that they can adapt themselves. Additional time seems necessary to ensure the proper development of harmonised standards, common specifications and/or the alignment of CSA schemes enabling the presumption of conformity for new category of critical products.	Where a new category of critical products with digital elements is added to the list in Annex III by means of a delegated act pursuant to paragraph 2 of this Article, it shall be subject to the relevant conformity assessment procedures referred to in Article 24(2) and (3) within ~~12~~ **24** months of the date of adoption of the related delegated act.
Highly critical products	ITRE	6(5)	50	The Commission is empowered to adopt delegated acts in accordance with 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 pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. ***The obligation to obtain***	Positive with comments	By providing a timeframe, this new provision enhances legal certainty for manufacturers. However, the timeframe may be too short for the manufacturers. According to the category targeting, 12 months may not be achievable. To correctly implement this obligation, the timeframe should be extended. Cybersecurity certificate developments and adaption depends on various factors, for instance in the case of the EUCC,	The obligation to obtain a European cybersecurity certificate shall apply **24** ~~12~~ months after the adoption of the relevant delegated act.

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				a European cybersecurity certificate shall apply 12 months after the adoption of the relevant delegated act. When determining such categories of highly critical products with digital elements, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is.		additional protection profiles shall be developed, the existing ones shall be adapted and recertified. A minimum 24 months seems more realistic.	
Highly critical products	ITRE	6(5)	264	~~***The Commission is empowered to adopt delegated acts in accordance with 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 pursuant to Regulation (EU) 2019/881 to demonstrate conformity with the essential requirements set out in Annex I, or parts thereof. When determining such categories of highly critical products with digital elements, the Commission shall take into account the level of cybersecurity risk related to the category of products with digital elements, in light of one or several of the criteria listed in paragraph 2, as well as in view of the assessment of whether that category of products is: (a) used or relied upon by the essential entities of the type referred to in Annex [Annex I] to the Directive [Directive XXX/ XXXX (NIS2)] or will have potential future significance for the activities of these entities; or (b) relevant for the resilience of the overall supply chain of products with digital elements against disruptive events.***~~	Negative	This article is essential to recognise the added value of EU cybersecurity certification, it ensures consistency with already certified products that are used in critical environment. Moreover, the assessment provided by Cybersecurity Act is more demanding than NLF modules applicable to class I and II and ensures product's robustness whiles NLF modules focuses more on correctness.	Keep the initial proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Highly critical products	ITRE	6(5)	266	***The Commission is empowered to adopt the delegated acts referred to in paragraph 5 of this Article no earlier than 12 months after the adoption of the relevant European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881***	Positive		
Expert group	ITRE	6(5)b new	52	***Before adopting the delegated acts referred to in paragraphs 2, 4 and 5 of this Article, the Commission shall consult the Expert Group referred to in [Article 6a]***	Positive	Stakeholder consultation should be the ground basis	**Additionally public consultation could be necessary if no representant of the category of product which will be impacted by the adoption of the delegated act are represented in the Expert Group.**
Expert group	ITRE	6a new	53	***By ... [6 months after the date of entry into force of this Regulation], the Commission shall establish an expert group on cyber resilience (the 'Expert Group'). The composition of the Expert Group shall aim to be gender and geographically balanced and shall include the following:*** ***(a) representatives of each of the following:*** ***(i) the European Union Agency for Cybersecurity;*** ***(ii) the European Data Protection Board;*** ***(iii) Europol;*** ***(iv) the European Defence Agency;*** ***(b) experts representing relevant private stakeholders, ensuring adequate representation of micro, small and medium sized enterprises;*** ***(c) experts representing civil society, including consumer organisations;***	Positive with comments	The proposal to establish an expert group is an interesting tool to collect feedback on the implementation of the CRA. Moreover, as cybersecurity is a matter of moving target, it is expected to continuously update end enhance the applicable standards, methodologies, and other means to demonstrate conformity with the essential requirements. From this perspective a holistic view from experts could be helpful. **On the composition of the Expert Group:** The CRA does not apply to products exclusively developed for military and national security purposes, therefore Europol and European Defence Agency participation is not relevant. Additionally, representatives from the European Standardisation Organisations and Member States (i.e. National Bodies), are missing.	By ... [6 months after the date of entry into force of this Regulation], the Commission shall establish an expert group on cyber resilience (the 'Expert Group'). The composition of the Expert Group shall aim to be gender and geographically balanced and shall include the following: (a) representatives of each of the following: (i) the European Union Agency for Cybersecurity; (ii) the European Data Protection Board; ***(iii) ~~Europol;~~ European Standardisation organisations*** ***(iv) ~~the European Defence Agency;~~ Member States*** ***(v) the European Cybersecurity Certification Group pursuant to Regulation (EU) 2019/881***

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				(d) experts appointed in a personal capacity, who have proven knowledge and experience in the areas covered by this Regulation; ***(e) experts representing academia, including universities, research institutes and other scientific organisations, including persons with global expertise.*** ***2. The Expert Group shall advise the Commission with regard to the following:*** ***(a) the list of critical products with digital elements set out in Annex III, as well as on the possible need to update that list;*** ***(b) the implementation of European cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 and on the possibility to make them mandatory for highly critical products with digital elements;*** ***(c) the elements of the Regulation to be addressed by the guidelines referred to in Article 17a;*** ***(d) the availability and the quality of European and international standards, and the possibility to supplement or replace them with common technical specifications;*** ***(e) the availability of skilled professionals in the field of cybersecurity across the Union, including of adequate personnel to perform third-party conformity assessments pursuant to this Regulation;*** ***(f) the possible need to amend this Regulation.*** ***The Expert Group shall also map trends at Union and Member State level regarding existing and patched vulnerabilities.***		**On the missions:** Implementation of cybersecurity schemes for highly critical products is mandatory and should not been discussed within this group. However, the maintenance of the scheme and the necessary Protection Profiles should be addressed per vertical. For this topic, ENISA, ECCG representatives and future maintenance organisation representatives are relevant. When it comes to the certification for highly critical products, since this certification is mandatory, the expert group is not entitled to advice on it. However, the group should be consulted regarding the type of products falling under this category and requiring a cybersecurity certification. Moreover, Mapping of trends regarding existing and patched vulnerability is in the remit of ENISA and national authorities, cooperation is already in place. On standards availability. When possible harmonised standards should be the privileged approach. However, as the CRA embrace a wide range of verticals, it seems reasonable to make the best use of the industrial and technical legacy in terms of "private standards / private common specifications" which could be easily translated into "common specifications". – to avoid any overinterpretation of the current mission, paragraph d shall be split into additional paragraphs (see proposal).	***(v) the stakeholder Cybersecurity Certification Group pursuant to Regulation (EU) 2019/881*** (b) experts representing ~~***relevant private stakeholders***~~***, Companies, manufacturers developers of products with digital elements including micro, small and medium sized enterprises, Business organisations,*** ensuring adequate ***sectorial*** representation ~~**of micro, small and medium sized enterprises;**~~ (c) experts representing civil society, including consumer organisations; ~~***(d) experts appointed in a personal capacity, who have proven knowledge and experience in the areas covered by this Regulation;***~~ ***Expert representing European and international fora and consortia active in the field of ICT standardisation and cybersecurity certification.*** (e) experts representing academia, including universities, research institutes and other scientific organisations, including persons with global expertise. 2. The Expert Group shall advise the Commission with regard to the following: (a) the list of critical products with digital elements set out in Annex III, as well as on the possible need to update that list;

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				3. The Expert Group shall take into account the views of a wide range of stakeholders. ***4. The Expert Group shall be chaired by the Commission and shall be constituted in accordance with the horizontal rules on the creation and operation of Commission expert groups. In that context, the Commission may invite experts with specific expertise on an ad hoc basis.*** ***5. The Expert Group shall carry out its tasks in accordance with the principle*** ***of transparency. The Commission shall publish a summary of the meetings of the Expert Group and other relevant documents on the Commission website***			(b) the ~~***implementation***~~ ***recognition*** of European cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 **to demonstrate conformity with the essential requirements or parts thereof as set out in Annex I,** and on **the possibility to identify new** ~~***make them mandatory for***~~ highly critical products with digital elements; (c) the elements of the Regulation to be addressed by the guidelines referred to in Article 17a; (d) the ***standardisation requests to the European Standardisation Organisations.*** ***( ) the development of*** ~~***availability and the quality of European and international standards, and the possibility to supplement or replace them with***~~ common technical specifications ***taking into account the availability and the quality of European, international and private standards.*** (e) the availability of skilled professionals in the field of cybersecurity across the Union, including of adequate personnel to perform third-party conformity assessments pursuant to this Regulation; (f) the possible need to amend this Regulation. ~~**The Expert Group shall also map trends at Union and Member State level regarding existing and patched vulnerabilities.**~~

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
							3. The Expert Group shall take into account the views of a wide range of stakeholders. 4. The Expert Group shall be chaired by the Commission and shall be constituted in accordance with the horizontal rules on the creation and operation of Commission expert groups. In that context, the Commission may invite experts with specific expertise on an ad hoc basis. 5. The Expert Group shall carry out its tasks in accordance with the principle of transparency. The Commission shall publish a summary of the meetings of the Expert Group and other relevant documents on the Commission website ***6. Advise in areas supporting the adoption, especially for SMEs/SMBs*** ***7. Advise NBs and CABs in their capability for handling the market demands and needs***
Public procurement	ITRE	9a (new)	54	***1. Without prejudice to Directives 2014/24/EU1 and 2014/25/EU of the European Parliament and of the Council, Member States shall ensure, when procuring products with digital elements, a high level of cybersecurity and appropriate expected product lifetimes.*** ***2. Member States shall ensure that manufacturers remedy vulnerabilities in publicly procured products with digital elements as a matter of urgency, including by making security updates available promptly.***	Negative	The CRA ensures an appropriate level of cybersecurity to all - including MS - as well as transparency regarding the expected lifetime. Therefore, this proposal is redundant. Regarding item (2), the CRA already ensures vulnerability handling of products with digital elements. In addition, market surveillance authorities already have the power to request prompt availability of security updates. Therefore there is no need to further require it in the course of public procurement.	Remove this provision

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Essential requirements	ITRE	10(1)	269	When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I. ***Manufacturers may deviate from a requirement in justified cases if it does not apply due to the nature of the product. Manufacturers should document the justification in the cybersecurity risks assessment in accordance to paragraph 2.***	Positive	Not all of requirements are applicable to each and every manufacturer's product.	Keep this proposal
Open source	ITRE	10(4)	55	For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements. ***When integrating components of open-source software that have not been placed on the market in the course of a commercial activity, manufacturers shall ensure that such components comply with this Regulation.***	Negative	This approach goes beyond due diligence and place the burden on manufacturer exclusively. It is neither an incentive for open-source software to develop robust products, neither a good choice for manufacturers that would be reluctant to bear both risk and liability.	Remove the new proposal while keeping the orginal provision
Open source	ITRE	10(4)		For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. ***It falls upon the manufacturer to*** ensure that such components do not compromise the security of the product with digital elements, ***in particular in the case of open source software that have not been placed on the market in exchange of financial or other type of monetisation, including data returns. The due diligence obligation can be considered fulfilled if all components have been already deemed compliant and the CE mark has been affixed to them as appropriate.***	Negative	This approach goes beyond due diligence and place the burden on manufacturer exclusively. It is neither an incentive for open-source software to develop robust products, neither a good choice for manufacturers that would be reluctant to bear both risk and liability.	Remove the new proposal while keeping the orginal provision

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Product lifetime and vulnerability handling	ITRE	10(6)1	56	When placing a product with digital elements on the market, ***manufacturers shall determine the expected product lifetime of those products. In doing so, the manufacturer shall ensure that*** the expected product lifetime ***is in line with reasonable consumer expectations and that it promotes sustainability and the need to ensure long-lasting products with digital elements.*** Manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I ***during at least the expected product lifetime. Where applicable, the expected product lifetime shall be clearly stated on the product, its packaging or be included in contractual agreements.***	Negative	This proposal considers that vulnerability handling can always be ensured over a product lifetime of 5 years which is not at all the case. For some technologies or types of products, it may be challenging for manufacturer to ensure sustainable and long-lasting products as the risks are constantly evolving and increasing. In these cases, while the level of resistance of the product with digital element can be estimated and committed by the manufacturer over a medium period of time (3-5 years) **starting from the development of the product with digital elements, or the placement on the market of the first item,** it is hardly possible to guarantee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development. Multiple examples demonstrate this situation. Depending on the technologies, types of product, the risks, and the criticality, the manufacturer may be able to commit for a more or less long lifetime, which in some cases may be below 5 years. The right approach is to ensure transparency for consumers. Product lifetime should be clearly indicated in the EU declaration of conformity, which is available to the consumer, so that the latter could make its choice in a fully informed manner. Therefore, the text should revert to the initial proposal from the European commission.	Revert to the initial proposal from the European commission.

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Information to users	ITRE	10(6)1	276	When placing a product with digital elements on the market, and for the expected product lifetime ***indicated by the manufacturer,*** or for a period of five years from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I. ***The Commission may, after consulting the Cyber Resilience Expert Group, ADCO, ENISA, and, where necessary, other relevant stakeholders, by means of implementing acts, specify the format and information of the label for consumer products with digital elements, which might easily indicate the expected lifetime of the product. On top of that, this label might contain additional information enabling consumers to quickly understand the level of security and privacy associated with the product. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).***	Negative	This call for transparency would be misleading for the consumer. This approach is mixing CE marks with Cybersecurity trust marks (which may also be provided on a national base, see e.g. BSI Cyber Security label in Germany). Moreover, CRA is only addressing transversal basic cybersecurity requirements which remains the same whatever the criticality is. The type of assessment is the only element which differentiate the products categories. Providing information to users on this basis could lead to overinterpretation of the product security functions.	Delete this proposal
Information to users	ITRE	10(6)2b	58	***Manufacturers shall actively inform users when their product with digital elements has reached the end of its expected product lifetime and vulnerability handling requirements cease to apply***	Negative	This requirement cannot be fulfilled for all products with digital elements, as many of them do not have any user interface (cards, routers, FPGA,...) on which the manufacturer could leverage to inform the user. In addition, the manufacturer does not usually know who bought its product with digital element and thus can't contact them. Instead, this information should be part of the EU declaration of conformity. The commission might consider a passive, rather than active, method giving those considerations. For example, a manufacturers portal where	Removal or clarify that this provision shall apply ***"when possible"***

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
						consumers can subscribe for receiving such notifications and the information is available with regards of the product specifics.	
Lifetime IP of manufacturer	ITRE	10(6)2c	59	***Where the expected product lifetime is shorter than five years and the handling of vulnerabilities has therefore ended in accordance with the vulnerability handling requirements set out in Section 2 of Annex I, manufacturers shall provide free access to the source code of such a product with digital elements to undertakings. Those undertakings shall commit to extending the provision of vulnerability handling services, in particular security updates. Access to such source codes shall be provided only where provided for in a contractual arrangement. Those arrangements shall protect the ownership of the product with digital elements and shall prevent the dissemination of the source code to the public. The obligation to provide free access to the source code shall cease to apply when the lifetime of the product has reached five years.***	Negative	This proposal considers that vulnerability handling can always be ensured over a product lifetime of 5 years which is not at all the case. For some technologies or types of products, it may be challenging for manufacturer to ensure sustainable and long-lasting products as the risks are constantly evolving and increasing. In these cases, while the level of resistance of the product with digital element can be estimated and committed by the manufacturer over a medium period of time (3-5 years) **starting from the development of the product with digital elements, or the placement on the market of the first item,** it is hardly possible to guarantuee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development. Multiple examples demonstrate this situation. Depending on the technologies, types of product, the risks, and the criticality, the manufacturer may be able to commit for a more or less long lifetime, which in some cases may be below 5 years. This proposal will not change that. Besides, the spirit of the amendment fails to address the fundamental issue as this scenario might imply that support cannot be longer given. For example, consumers having access to source code might be contra productive if there is not support given and modifications are driven by assumptions". Finally , this proposal substantially harms the manufacturer as it obliges him to	Remove this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
						disclose sensitive IP (patents, know how,...) which may ultimately put at risk its existence.	
Standards	ITRE	10(9)	288	Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in conformity. The manufacturer shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised or ***international standards***, European cybersecurity certification schemes or the common specifications referred to in Article 19 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified. ***Where new knowledge, techniques, or standards become available, which were not available at the time of design of a serial product, the manufacturer may consider implementing such improvements for future product generations. The manufacturer shall take into account the associated costs and efforts, including the efforts required for development, testing, validation and approval process time.***	Negative	This proposal conflicts with current harmonised standards, common specification and European certification schemes' updating processes. Moreover, international standards cannot be implemented as such, Vienna and Frankfort agreements provide the elements for CEN/CENELEC to translate them into the European standardisation framework.	Remove this proposal
Lifetime	ITRE	10(12)	62	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 are 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	Negative	The original proposal from the Commission should be kept as it better takes into account the reality of cybersecurity products. For some technologies or types of products, it may be challenging for manufacturer to ensure sustainable and long-lasting products as the risks are constantly evolving and increasing. In these cases, while the level of resistance of the product with digital element can be estimated and guaranteed by the	Revert to the initial proposal from the European commission.

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.		manufacturer over a medium period of time (3-5 years) **starting from the development of the product with digital elements, or the placement on the market of the first item,** it is hardly possible to guarantuee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development. Multiple examples demonstrate this situation. Depending on the technologies, types of product, the risks, and the criticality, the manufacturer may be able to guarantee a more or less long lifetime, which in some cases may be below 5 years. Therefore, the text should revert to the initial proposal from the European commission.	
SBOM	ITRE	10(15)	300	The Commission may, by means of implementing acts, ***and following an open consultation with stakeholders and in line with international standards***, specify the format and elements of the software bill of materials set out in Section 2, point (1), of Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2)	Neutral	Industry consultation is a good approach, however detailed SBOM format is necessary to ensure the applicability of the CRA. These elements should be defined ahead in advance of the entry into force of this regulation.	
Reporting obligations – patched vulnerability	ITRE	11(1)	309	The manufacturer shall, without undue delay and in any event within 72 hours ***after the patch is publicly available***, notify to ***CSIRT Network any new patched vulnerabilities*** contained in the product with digital elements ***that may be actively exploited and pose a significant cybersecurity risk.*** The notification shall include basic details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken	Positive with comments	Reporting of patch vulnerabilities related to products with digital elements that may be actively exploited and pose a significant cybersecurity risk is a much more realistic approach.	Keep this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				based on the manufacturers coordinated vulnerability disclosure ***policy required by section 2 of Annex I item (5) (e.g., the ISO/IEC 29147).***			
Reporting obligations – actively exploited vulnerability	ITRE	11(1)	64 307	The manufacturer shall notify, ~~***without undue delay and in any event within 24 hours of becoming aware of it,***~~ to ENISA any actively exploited vulnerability contained in the product with digital elements~~***. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken***~~ ***in accordance with paragraph 1a of this Article***. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notification to the CSIRT designated for the purposes of coordinated vulnerability disclosure in accordance with Article [Article X] of ***Directive (EU) 2022/2555*** of Member States concerned upon receipt and inform the market surveillance authority about the notified vulnerability. ***Where a notified vulnerability has no corrective or mitigating measures available, ENISA shall ensure that information about the notified vulnerability is shared in line with strict security protocols and on a need-to-know-basis***	Positive	The notification process is much more realistic thanks to the proposed notification procedure. This procedure leaves more time for manufacturers to gather information and carry out the needed analysis. Introduction of need-to-know principle for the disclosure of vulnerabilities which can't be corrected or mitigated.	Keep this proposal
Reporting obligations – actively exploited vulnerability	ITRE	11(1a) (new)	65	***1a. Notifications as referred to in paragraph 1 shall be subject to the following procedure:*** ***(a) an early warning, without undue delay and in any event within 24 hours of the manufacturer becoming aware of the actively exploited vulnerability, detailing whether any known corrective or mitigating measure is available;***	Positive	A final report within one month is not always realistic. For some products there may be no update available or corrective action. Consider the scenario where fixing a vulnerability requires development or support from parties outside the control of the manufacturer. On top of it, the manufacturer can help users to navigate the risks until a final solution is available. Considerations should be made to support this scenario,	Keep this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				(b) a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which, where applicable, updates the information referred to in point (a), details any corrective or mitigating measures taken and indicates an assessment of extent of the vulnerability, including its severity and impact; ***(c) an intermediate report on relevant status updates, upon the request of ENISA;*** ***(d) a final report, within one month after the submission of the vulnerability notification under point (b), including at least the following:*** ***(i) a detailed description of the vulnerability, including its severity and impact;*** ***(ii) where available, information concerning any actor that has exploited or that is exploiting the vulnerability;*** ***(iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.***		like for example intermediate reports (e.g. every month) and then a final report when a solution is available. Clarifications are brought regarding notification process. In addition, this procedure leaves more time for manufacturers to gather information and carry out the needed analysis. Need deeper analysis for reporting obligation for a supply chain perspective: CRA only address from a product perspective – guidance would be necessary. When it comes to the applicability for product with digital elements that have been certified (EUCC EUCS etc.), a deeper analysis would be align the reporting obligation from a scheme perspective.	
Reporting obligations – incident	ITRE	11(2)	67	The manufacturer shall ~~***without undue delay and in any event within 24 hours of becoming aware of it,***~~ notify to ENISA any ***significant*** incident having impact on the security of the product with digital elements ***in accordance with paragraph 2b of this Article***. ENISA shall, without undue delay, unless for justified cybersecurity risk-related grounds, forward the notifications to the single point of contact designated in accordance with Article [Article X] of ***Directive (EU) 2022/2555*** of the Member	Positive	Only **significant incidents** should be reported on a mandatory basis, in alignment with NIS 2. It alleviates the burden for manufacturer and ensures that only relevant and useful information about incidents are notified. In addition this proposal clarifies that the notification does not entail increased liability for the manufacturer.	Keep this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				States concerned and inform the market surveillance authority about the notified ***significant*** incidents. The ~~***incident***~~ ***mere act of*** notification shall ~~***include information on the severity and impact of the incident and, where applicable, indicate whether the manufacturer suspects the incident to be caused by unlawful or malicious acts or considers it to have a cross-border impact***~~ ***not subject the notifying entity to increased liability***			
Reporting obligations - incident	ITRE	11(2)(a) (new)	68 317	***An incident shall be considered to be significant as referred to in paragraph 2, where:*** ***(a) it has caused or is capable of causing severe operational disruption of the production or the services for the manufacturer concerned, which would impact the security of a product; or*** ***(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.***	Positive	It clarifies the meaning of significant incident.	Keep this proposal
Reporting obligations - incident	ITRE	11(2)b	69	***Notifications as referred to in paragraph 2 shall be subject to the following procedure:*** ***(a) an early warning, without undue delay and in any event within 24 hours of the manufacturer becoming aware of the significant incident, which, where applicable, indicates whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;*** ***(b) an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the significant incident, which, where applicable, updates the information referred to in point (a) and indicates an***	Positive	A final report within one month is not always realistic. For some products there may be no update available or corrective action. Consider the scenario where fixing a vulnerability requires development or support from parties outside the control of the manufacturer. On top of it, the manufacturer can help users to navigate the risks until a final solution is available. Considerations should be made to support this scenario, like for example intermediate reports (e.g. every month) and then a final report when a solution is available. Clarifications are brought regarding notification procedure.	Keep this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise; ***(c) an intermediate report on relevant status updates upon the request of ENISA;*** ***(d) a final report, within one month after the submission of the incident notification under point (b), including at least the following:*** ***(i) a detailed description of the incident, including its severity and impact;*** ***(ii) the type of threat or root cause that is likely to have triggered the incident;*** ***(iii) applied and ongoing mitigation measures;*** ***(iv) where applicable, the cross-border impact of the incident;*** ***In the event of an ongoing incident at the time of the submission of the final report referred to in point (d) of the first subparagraph, Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.***		In addition, this procedure leaves more time for manufacturers to gather information and carry out the needed analysis. When it comes to the applicability for product with digital elements that have been certified (EUCC EUCS etc.), a deeper analysis would be align the reporting obligation from a scheme perspective.	
Reporting obligations - incident	ITRE	11(4)	70	The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the ***significant*** incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the ***significant*** incident	Positive with comments	Only significant incidents should be reported. It alleviates the burden for manufacturer and ensures that only relevant and useful information about incidents is notified. However, the amendment should acknowledge that manufacturers often doesn't know who the users are. Passing this activity down to the supply chain makes no difference as well.	The manufacturer shall ***provide mechanism to inform***, without undue delay and after becoming aware, the users of the product with digital elements about the *significant* incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the *significant* incident

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Reporting obligations – voluntary reporting	ITRE	11(a) new	74	***Voluntary reporting*** ***1. In addition to the notification obligations set out in Article 11, notifications may be submitted to ENISA on a voluntary basis by the following:*** ***(a) manufacturers, with regard to incidents, cyber threats and near misses;*** ***(b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Regulation, with regard to significant and non-significant incidents, cyber threats and near misses;*** ***(c) any actor with regard to vulnerabilities which may be included in the European vulnerability database referred to in Article 12 of Regulation 2022/255.*** ***2. ENISA shall process the notifications referred to in paragraph 1a of this Article in accordance with the procedure laid down in Article 11. ENISA may prioritise the processing of mandatory notifications over voluntary notifications.*** ***3. Where appropriate, ENISA shall ensure the confidentiality and appropriate protection of the information provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.***	Neutral	The benefit of this proposal is to provide a legal framework for voluntary reporting.	
Distributor	ITRE	14(3)	75	Where a distributor considers or has reason to believe, ***on the basis of information in their possession,*** that a product with digital elements or the processes put in place by the manufacturer are not in conformity	Positive	The distributor doesn't have access to the same information regarding the product with digital elements as the manufacturer and can only take such	Keep this proposal The same provision should also apply to importer in article 13(3).

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				with the essential requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform the manufacturer and the market surveillance authorities to that effect.		decisions on the ground of the information in its possession. Moreover, the same provision should also apply to importer in article 13(3).	
Distributor	ITRE	14(4)	76	Distributors who know or have reason to believe, on the basis of information in their possession, 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.	Positive	The distributor doesn't have access to the same information regarding the product with digital elements as the manufacturer, and can only take such decisions on the ground of the information in its possession. However the same provision should also apply to importer in article 13.6.	Keep this proposal. The same provision should also apply to importer in article 13(6)
Distributor	ITRE	14(6)	77	***On the basis of information in their possession***, when the distributor of a product with digital elements becomes aware that the manufacturer of that product ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market	Positive	The distributor doesn't have access to the same information regarding the product with digital elements as the manufacturer and can only take such decisions on the ground of the information in its possession. However, the same provision should also apply to importer in article 13.9.	Keep this proposal. The same provision should also apply to importer in article 13(9)

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Guidelines	ITRE	17(a) new	78	***Article 17a Guidelines*** ***1. In order to create clarity and certainty for and consistency among the practices of economic operators, the Commission shall prepare and issue guidelines in the form of a handbook for economic operators, explaining how to apply this Regulation, with a particular focus on how to facilitate compliance by micro, small and medium-sized enterprises.*** ***2. The guidelines shall be published by ... [12 months after the entry into force of this Regulation] and shall be regularly updated, in particular in light of potential amendments to the list of critical products set out in Annex III. They shall contain at least the following elements:*** ***(a) a detailed explanation of the scope of this Regulation, outlining the impact on the various sectors of the Union's economy;*** ***(b) clear and descriptive examples of remote data processing solutions designed and developed by or on behalf of the manufacturer ;*** ***(c) information to determine what constitutes a commercial activity for free and open-source software developers;*** ***(d) a detailed description of the methodology employed to distinguish between critical products with digital elements of classes I and II;*** ***(e) a clear illustration of the interaction between this Regulation and other Union law, particularly concerning presumptions of conformity and conformity assessments;*** ***(f) guidance for manufacturers on how to perform the cybersecurity risk***	Positive	We disagree with point (g) as the expected lifetime should be freely determined by the manufacturer based on its technical capacities. The original proposal from the Commission should be kept as it better takes into account the reality of cybersecurity products. For some technologies or types of products, it may be challenging for manufacturer to ensure sustainable and long-lasting products as the risks are constantly evolving and increasing. In these cases, while the level of resistance of the product with digital element can be estimated and guaranteed by the manufacturer over a medium period of time (3-5 years) **starting from the development of the product with digital elements, or the placement on the market of the first item,** it is hardly possible to guarantuee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development. Multiple examples demonstrate this situation. Depending on the technologies, types of product, the risks, and the criticality, the manufacturer may be able to guarantee a more or less long lifetime, which in some cases may be below 5 years.	Keep this proposal except bullet (g) which should be removed.

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				assessment referred to in Article 10(2) and an explanation of how the risk assessment affects manufacturers' compliance with the essential requirements of this Regulation; ***(g) guidance for manufacturers on how to determine appropriately the expected product lifetime, with an adequate level of product granularity;*** ***(h) an explanation of how to handle reporting requirements pursuant to this Regulation or to other Union law;*** ***(i) an overview of the Commission's empowerments to adopt delegated and implementing acts, with the relevant deadlines, where appropriate.*** ***3. When preparing the guidelines pursuant to this Article, the Commission shall consult the Expert Group.***			
Common Specifications	ITRE	19(1)	79	***The Commission is empowered to adopt delegated acts in accordance with Article 50 to establish common specifications that cover technical requirements providing a means to comply with the requirements set out in Annex I for products within the scope of this Regulation where the following conditions have been fulfilled*** ***(a)*** the Commission has ***requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more*** European standardisation organisations ***to draft a harmonised standard for*** the essential requirements set out in Annex ***I and the request has not been accepted or the European standardisation deliverables addressing that request is not***	Negative	Regarding the approach where common specification should be seen as a last-resort option, we disagree. Common specifications may also be very useful to leverage existing industry or sector specific standards for which it has been demonstrated that they meet some or all of the essential requirements of Annex I. As such, common specification could support a quick implementation of the CRA, while limiting the impact on the industry. In this case the adoption of common specifications shall not be bound to the failure of standardisation requests. Besides the standardisation legacy from the private sector, common specifications would be the key tool to recognise Protection Profiles from the EUCC scheme as sectorial approach to	Revert to the proposal of the European Commission.

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				delivered within the deadline set in accordance with ***Article 10(1) of Regulation (EU) No 1025/2012 or European standardisation deliverables do not comply with the request; and*** ***(b) no reference to harmonised standards covering the relevant essential requirements set out in Annex I is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.*** ***2. Before preparing the delegated act, the Commission shall inform the Expert Group that it considers that the conditions in paragraph 1 are fulfilled. In preparing the delegated acts, the Commission shall take into account the opinions of the Expert Group*** ***3. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the publication of its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference to a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal the relevant delegated acts referred to in paragraph 1, or the parts thereof which cover the same essential requirements set out in Annex I.***		demonstrate conformity with the CRA's essential requirements.	

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Obligation – technical documentation	ITRE	23(2)	81	The technical documentation shall be drawn up before the product with digital elements is placed on the market and shall be continuously updated, where appropriate, during the expected product lifetime ~~***or during a period of five years after the placing on the market of a product with digital elements, whichever is shorter.***~~	Negative	The original proposal from the EC should be kept as it better takes into account the reality of cybersecurity products. For some technologies or types of products, it may be challenging for manufacturer to ensure sustainable and long-lasting products as the risks are constantly evolving and increasing. In these cases, while the level of resistance of the product with digital element can be estimated and guaranteed by the manufacturer over a range of time (3-5 years) **starting from the development of the product with digital elements, or the placement on the market of the first item,** it is hardly possible to guarantee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development. Multiple examples demonstrate this situation. Depending on the technologies, types of product, the risks, and the criticality, the manufacturer may be able to commit for a more or less long lifetime, which in some cases may be below 5 years.	Revert to the proposal of the European Commission.
Presumption of conformity	ITRE	24(2)a	83	***Harmonised standards, common specifications or European cybersecurity certification schemes shall be in place for six months before the conformity assessment procedure referred to in paragraph 2 applies. In the six months prior to the application of paragraph 2, or where, due to a cause clearly attributable to the Commission, harmonised standards, common specifications or European cybersecurity certification schemes do not exist, manufacturers shall demonstrate the conformity of the critical product with digital elements of Class I as set out in***	Negative	1/ Other methods than hEN, Common specifications or European cybersecurity certification scheme can always be used for the conformity assessment of product with digital elements (e.g. internal specification). In that case however, conformity with annex I must be demonstrated. 2/If the absence of such items is a problem for the conformity assessment of class I product, likewise it should be a problem for non-critical product with digital elements.	Remove this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				Annex III via the procedure referred to in paragraph 1.		3/ And what about class II product? For which reason only class I are considered? This proposal may create substantial confusions amongst Notified Bodies and thus should be removed.	
Mutual recognition and international standards	ITRE	24 a (new)	85	***Mutual recognition agreements*** ***1. In order to promote international trade, the Commission shall endeavour to conclude Mutual Recognition Agreements (MRAs) with like-minded third countries. MRAs shall be established only between the Union and third countries that are on a comparable level of technical development and have a compatible approach concerning conformity assessment. They shall ensure the same level of protection as that provided for by this Regulation.*** ***2. The Commission shall assess international standards and evaluate whether they provide the same level of protection as the one provided for by this Regulation, with the aim to simplify the development of harmonised European standards.***	Positive with comments	Rely on Recital 67 of the original proposal. Criteria for mutual recognition shall be clarified.	Mutual recognition agreements 1. In order to promote international trade, the Commission shall endeavour to conclude Mutual Recognition Agreements (MRAs) with ~~***like-minded***~~ third countries. MRAs shall be established only between the Union and third countries that are on a comparable level of technical development and have a compatible approach concerning conformity assessment. They shall ensure the same level of protection as that provided for by this Regulation. ***MRAs shall be based on the mutual acceptance of certificates, marks of conformity and test reports issued by the conformity assessment bodies of either party in conformity with the legislation of the other party.*** ***2. The Commission shall assess international standards and evaluate whether they provide the same level of protection as the one provided for by this Regulation, with the aim to simplify the development of harmonised European standards.***
Product lifetime	ITRE	41 (9)a (new)	89	***9a. Market surveillance authorities shall provide the Commission with data about the average expected product lifetime set by the manufacturers, disaggregated per category of product with digital elements. The Commission***	Negative	The expected lifetime should be freely determined by the manufacturer based on its technical capacities. For some technologies or types of products, it may be challenging for manufacturer to ensure sustainable and	Remove this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				shall publish that information in a publicly accessible and user-friendly database.		long-lasting products as the risks are constantly evolving and increasing. In these cases, while the level of resistance of the product with digital element can be estimated and guaranteed by the manufacturer over a medium period of time (3-5 years) **starting from the development of the product with digital elements, or the placement on the market of the first item,** it is hardly possible to guarantee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development. Multiple examples demonstrate this situation. Depending on the technologies, types of product, the risks, and the criticality, the manufacturer may be able to guarantee a more or less long lifetime, which in some cases may be below 5 years.	
Market surveillance	ITRE	45 (1)	90	Where the Commission has sufficient reasons to consider, including based on information provided by ENISA, that a product with digital elements that presents a significant cybersecurity risk is non-compliant with the requirements laid down in this Regulation, it ~~***may***~~ ***shall*** request the relevant market surveillance authorities to carry out an evaluation of compliance and follow the procedures referred to in Article 43.	Negative	Strongly recommend the Commission to consider the resources.	Stick to the initial proposal
Market surveillance	ITRE	45 (2)	91	In exceptional circumstances which justify an immediate intervention to preserve the good functioning of the internal market and where the Commission has sufficient reasons to consider that the product referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective	Negative	Strongly recommend the Commission to consider the resources.	Stick to the initial proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				measures have been taken by the relevant market surveillance authorities, the Commission ~~***may***~~ ***shall*** request ENISA to carry out an evaluation of compliance. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.			
Market surveillance	ITRE	48(1)	92	Market surveillance ~~authorities ***may agree with other relevant authorities to***~~ ***shall*** carry out joint activities aimed at ensuring cybersecurity and protection of consumers with respect to specific products with digital elements placed or made available on the market, in particular products that are often found to present cybersecurity risks.	Positive with comments	Good approach, however, need criteria to focus on "product that are often found to present cybersecurity risks" and objectives. Moreover, should be a possibility not an obligation to market surveillance authorities whilst considering their resources.	
Market surveillance	ITRE	48(2)	93	The Commission or ENISA ~~***may***~~ ***shall*** propose joint activities for checking compliance with this Regulation to be conducted by market surveillance authorities based on indications or information of potential non-compliance across several Member States of products falling in the scope of this Regulation with the requirements laid down by the latter.	Negative	Strongly recommend the co-legislators to consider the resources and clearly define the objectives.	
Market surveillance - sweeps	ITRE	49(1)	94	Market surveillance authorities ~~***may decide to***~~ ***shall regularly*** conduct simultaneous coordinated control actions ("sweeps") of particular products with digital elements or categories thereof to check compliance with or to detect infringements to this Regulation. ***Such sweeps shall prioritise products with digital elements placed on the market by manufacturers that may***	Positive with comments	Efforts should be put first on products with digital elements placed on the market by manufacturers that may put at risk the security of the Union. Strongly recommend the co-legislators to consider the resources and clearly define the objectives. e.g. market	Market surveillance authorities ***may decide to*** ~~***shall regularly***~~ conduct simultaneous coordinated control actions ("sweeps") of particular products with digital elements or categories thereof to check compliance with or to detect infringements to this Regulation. Such sweeps shall prioritise products

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				present a security risk for the Union. They shall include inspections of products acquired under a cover identity and shall aim to verify the compliance of those products with this Regulation, in particular with regard to identifying potential embedded backdoors or other exploitable vulnerabilities		surveillance authorities, shall sample annually a minimum of X% of the products In addition, sweeps operation should also target in priority products with digital whose conformity assessment procedure does not provide a high level of assurance regarding absence of vulnerability. While EU CSA security certification ensure a high level of trust in the security assessment of the product, it may not necessarily the case where Module A, Module B+C or Module H are used. Therefore, sweeps operation should target in priority product with digital elements whose conformity assessment relies on Module A, Module B+C and Module H.	with digital elements placed on the market by manufacturers that may present a security risk for the Union ***and products with digital elements whose conformity is not related to a third-party assessment.*** They shall include inspections of products acquired under a cover identity and shall aim to verify the compliance of those products with this Regulation, in particular with regard to identifying potential embedded backdoors or other exploitable vulnerabilities
Allocation of the revenue from the penalties	ITRE	53a (new)	103	***Allocation of the revenue from the penalties to support cybersecurity in the Union*** ***1. The revenue from the penalties referred to in Article 53(1) shall be allocated to projects raising the level of cybersecurity within the Union. Those projects shall aim to:*** ***(i) increase the number of skilled professionals in the field of cybersecurity;*** ***(ii) enhance capacity-building for micro, small and medium-sized enterprises in order to enable them to better comply with this Regulation;*** ***(iii) improve collective situational awareness of cyber threats;*** ***(iv) develop tools to increase the resilience of Union undertakings to cyber-enabled intellectual property theft.*** ***2. The revenue referred to in paragraph 1 shall be allocated to the Digital Europe Programme referred to in Article 6 of Regulation (EU) 2021/694. It***	Positive with comments	It should be clarified what will happen to the provision (2) when Digital Europe Programme will be completed.	Keep this proposal. Clarify what will happen to the provision (2) when Digital Europe Programme will be completed.

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				shall be earmarked to improve the cybersecurity of the Union. It shall constitute externally assigned revenue in accordance with Article 21(5) of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council1 and shall be implemented in accordance with the rules applicable to the Digital Europe Programme. It shall be considered to be a budgetary top-up and shall not be used to decrease the contribution from the Union budget. 3. The Commission is empowered to adopt delegated acts in accordance with Article 50 to supplement this Regulation concerning the modalities for the payment of the penalties referred to in Article 53.			
Entry into force	ITRE	55(3) a (new)	104	***Until ... [40 months after the date of entry into force of this Regulation], manufacturers may comply with the requirements of this Regulation on a voluntary basis. Where manufacturers comply with this Regulation with regard to their products with digital elements, they shall be considered also to comply with Delegated Regulation (EU) 2022/30.*** ***After ... [40 months after the date of entry into force of this Regulation, the Commission shall repeal Commission Delegated Regulation (EU) 2022/30.***	Positive	This provision would allow a smooth transition for manufacturers from the RED to the CRA regarding cybersecurity requirements, while alleviating their burden.	Keep this proposal
Entry into force	ITRE	57(2)	106	It shall apply from ... [~~***24***~~ ***40*** months after the date of entry into force of this Regulation]. However Article 11 (reporting obligations) shall apply from [~~***12***~~ ***20*** months after the date of entry into force of this Regulation].	Positive with comments	This provision gives more time to economic operators to get ready for the implementation of the CRA. However more time seems necessary as the CRA will have substantial impacts for economic operators.	It shall apply from ... [~~***24***~~ ***40*** months after the date of entry into force of ~~this Regulation~~ ***of delegated acts in accordance with Article 6(4) on the definition of products with digital elements' classes and of implementing acts in accordance with Article 10(15) on the format and elements of the SBOM.***

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
						To be applicable and to ensure legal certainty, definitions are necessary. - The Commission shall provide the definition of the products category, - The necessary element and format of the SBOM These elements should be defined ahead in advance of the entry into force of this regulation. Moreover, to ensure the correct activation of the provisions laid down in article 11, issuance of the implementing acts (art. 11(5)) regarding the type of information, format and procedure of the notification are necessary.	However Article 11 (reporting obligations) shall apply from [~~***12***~~ ***20*** months after the date of entry into force ~~of this Regulation~~ of implementing acts under Article 11.5].
Essential cybersecurity requirements	ITRE	Annex I - Part 1 - 3(a)(new)	108	be delivered without known exploitable vulnerabilities;	Positive	It is not realistic to require a product to be delivered without any vulnerabilities as a product with digital elements is always vulnerable. It is only a matter of time, will and money for attackers. Conversely, it is accurate to talk and only consider exploitable vulnerabilities, which we very much welcome. Besides, it doesn't reflect the State Of The Art in the industry where is not the existence of vulnerabilities but the potential exploitation of such vulnerabilities what counts. For example, a product may have no protection against local attacks and thus have exploitable attacks. However it is to be used in a datacentre where no malicious people can have access, or it may be a router in a family home where no one else than the family has access. In that	Keep this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
						scenario, this “exploitable vulnerability” is not an issue.	
Essential cybersecurity requirements	ITRE	Annex I - Part 1 - 3(a)	109	(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state ***while retaining all security updates;***	Positive	This proposal clarifies that past updates should be maintained	Keep this proposal
Product categories	ITRE	Annex III - Part I - (22)	113	Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC), ***industrial robots and their control systems, mobile machinery*** and supervisory control and data acquisition systems (SCADA);	Negative	The rationale for downgrading “industrial robots and their control systems, mobile machinery” from Class II to Class I is unclear. Yet, a cybersecurity attack on these products may have very substantial consequences. These products should be classified as class II.	Remove this proposal
Financial means for ENISA	ITRE	Annex VI a (new)	123	Capacity needs of the European Union Agency for Cybersecurity (ENISA) In order to fulfil its obligations under this Regulation and in order not to compromise existing obligations of the Agency under other Union law, the adequate staffing and financing of ENISA shall be ensured. Therefore additional tasks for ENISA under this Regulation shall be accompanied by additional human and financial resources. 8,5 additional full-time posts and corresponding additional appropriations will be needed to cover the additional tasks under this Regulation.	Positive	Means of ENISA should be reinforced to support the implementation of the CRA	Keep this proposal
Definition	IMCO	3(26)	8	***‘reasonably foreseeable misuse’ means the use of a product with digital elements in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems;***	Negative	This concept is important when drawing the information and instruction to the user as described in Annex II. It allows drawing the attention on the user on the cybersecurity risks that may result from any misuse	Keep the original proposal from the Commission

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Definition	IMCO	3(31)	9	substantial modification' means a change to the product with digital elements ***excluding security and maintenance updates*** following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Section 1 of Annex I or results in a modification to the intended use for which the product with digital elements has been assessed	Positive	This proposal acknowledges that security updates and maintenance as required by Annex I should not be considered as a substantial modification	Keep this proposal
Scope	IMCO	4(3a) (new)	11	***This Regulation shall not prevent Member States from subjecting products with digital elements to additional measures when these specific products will be used for military, defence or national security purposes, and such measures are necessary and proportionate for achievement of those purposes.***	Negative	Pursuant to article 2(5), products with digital elements developed exclusively for national security or military purposes are excluded from the scope of the CRA.	Remove this proposal
Components	IMCO	6(1)	12	Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. ***Only*** products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as falling into that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products. ***Integrating a component of higher class of criticality into a product of lower criticality does not change the level of criticality for the product the component is integrated into.***	Positive	This proposal clarifies the rules to apply in case of composition of a component in a products with digital elements	Keep this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Components	IMCO	10(4)	15	For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties in products with digital elements. They shall ensure that such components do not compromise the security of the product with digital elements ***and that the appropriate conformity assessment procedure has been carried out by the components manufacturers.***	Negative	This proposal seems useless and may substantially harm manufacturers. If the component is supplied from another manufacturer, it will fall under the scope of the CRA and thus will go through the conformity assessment procedure defined in article 24. Conversely, if the component is developed and supplied internally by the manufacturer, it should not be required to carry out a conformity assessment procedure pursuant to the CRA. Only the conformity assessment procedure performed on the final product with digital elements - which will be effectively placed on the market - should suffice.	Remove this proposal - Keep the original proposal from the Commission
Components	IMCO	10(4a) (new)	16	***The components manufacturers shall provide the information and documentation necessary to comply with the requirements of this Regulation, when supplying such components to the manufacturer of finished products. This informations shall be provided free of charge***	Positive	This proposal will ensure that the manufacturer has all the necessary technical documentation about the component.	Keep this proposal
Product lifetime	IMCO	10(6)	17	When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever ***is longer***, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I, ***provided that it is within the manufacturer's control.***	Negative	The expected lifetime should be freely determined by the manufacturer based on its technical capacities. For some technologies or types of products, it may be challenging for manufacturer to ensure sustainable and long-lasting products as the risks are constantly evolving and increasing. In these cases, while the level of resistance of the product with digital element can be estimated and guaranteed by the manufacturer over a medium period of time (3-5 years) **starting from the development of the product with digital elements, or the placement on the**	Revert to the proposal of the European Commission.

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
						market of the first item, it is hardly possible to guarantuee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development. Multiple examples demonstrate this situation. Depending on the technologies, types of product, the risks, and the criticality, the manufacturer may be able to guarantee a more or less long lifetime, which in some cases may be below 5 years.	
Manufacturer	IMCO	10(6)	17	When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is ***longer***, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I, ***provided that it is within the manufacturer's control.***	Positive	Regarding the second modification, it is very positive. It acknowledges two key aspects: • in the case where a product with digital element is integrated within another product with digital element, the vulnerability management may not be in the hand of the manufacturer of the first product with digital element, but rather in the hand of the one that integrated it; • the vulnerability handling also relies on the connectivity of the product with digital element, which is under control of the user, as well as its cooperation.	Keep this proposal
Conformity assessment	IMCO	10(7)3a (new)	18	***Where software updates are implemented,*** ***the manufacturer shall not be required to carry out another conformity assessment of the product with digital elements, unless the software update results in a substantial modification of the product with digital elements within the meaning of Article 3(31) of this Regulation.***	Positive	This proposal acknowledges that security updates and maintenance should not lead to another conformity assessment	Keep this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Product lifetime	IMCO	10(12)	20	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 longer***, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are 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	Negative	The expected lifetime should be freely determined by the manufacturer based on its technical capacities. For some technologies or types of products, it may be challenging for manufacturer to ensure sustainable and long-lasting products as the risks are constantly evolving and increasing. In these cases, while the level of resistance of the product with digital element can be estimated and guaranteed by the manufacturer over a range of time (3-5 years) **starting from the development of the product with digital elements, or the placement on the market of the first item,** it is hardly possible to guarantuee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development. Multiple examples demonstrate this situation. Depending on the technologies, types of product, the risks, and the criticality, the manufacturer may be able to guarantee a more or less long lifetime, which in some cases may be below 5 years. Regarding the second modification, -the vulnerability handling also relies on the connectivity of the product with digital element, which is under control of the user, as well as its cooperation.	Revert to the proposal of the European Commission.
Reporting obligations - vulnerabilities	IMCO	11(1)	21	The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify ENISA, by means of ***an early warning***, of any actively exploited vulnerability contained in the product with digital elements.	Positive with comments	This proposal acknowledges that the manufacturer needs time to gather and collect technical details and carry out minimum analysis regarding an actively exploited vulnerability.	The manufacturer shall, without undue delay and in any event within 24 hours of becoming aware of it, notify ENISA, by means of ***an early warning***, of any actively exploited vulnerability contained in the product with digital elements.

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
Reporting obligations - incidents	IMCO	11(4)	23	The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the ***significant*** incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the ***significant*** incident	Positive with comments	Only significant incidents should be reported. It alleviates the burden for manufacturer and ensures that only relevant and useful information about incidents is notified. However, a definition of **"significant"** should also be provided (refer to Amd 68 from ITRE draft report). However, the amendment should acknowledge that manufacturers often doesn't know who the users are. Passing this activity down to the supply chain makes not difference as well.	The manufacturer shall provide mechanism to inform, without undue delay and after becoming aware, the users of the product with digital elements about the ***significant*** incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the ***significant*** incident A definition of "significant" should also be provided. (refer to the amendment 68 from ITRE draft report)
Reporting obligations	IMCO	11(4a) (new)	24	***The obligations laid down in paragraphs 1, 2 and 4 will apply during the product lifetime. During the minimum product lifetime period the manufacturer will provide security updates for free, which will apply only to products with digital elements for which the manufacturer has drawn up an EU declaration of conformity, in accordance with Article 20 of this Regulation.***	Positive with comments	The obligation enacted in article 11 currently do not have any limit in time, which means that these obligations are endless. Manufacturer will have to abide by these provisions even if the product with digital elements is not sold anymore or has been withdrawn or recalled. It creates unnecessary burden for manufacturer which may impede their financial and innovation capacities. However, it is necessary to define the "minimum product lifetime".	Need to refer to the "minimum product lifetime" to be defined by the co-legislators.
Reporting obligations	IMCO	11(5)	25	The Commission may, by means of implementing acts, specify further the type of information, format and procedure of the notifications submitted pursuant to	Negative	By referencing this ISO standard, the regulation would not be technology neutral and would discard innovation.	Remove this proposal or reference the standards as an example in the referenced context

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				paragraphs 1 and 2. Those implementing acts shall ***be based on standard ISO/IEC 29157*** and shall be adopted in accordance with the examination procedure referred to in Article 51(2).		Moreover ISO/IEC 29157:2015 Information technology — addresses Telecommunications and information exchange between systems — PHY/MAC specifications for short-range wireless low-rate applications in the ISM band, which makes difficult to make the connection with the initial paragraph.	
Importer	IMCO	13(3)	31	Where an importer considers or has reason to believe, ***on the basis of the information at their disposal***, that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential requirements set out in Annex I, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with the essential requirements set out in Annex I. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect.	Positive	The importer doesn't have access to the same information regarding the product with digital elements as the manufacturer and can only take such decisions on the ground of the information in its possession. However the same provision should also apply to: • importer in article 13(6) and 13(9) • distributor in article 14(3), 14(4) and 14(6), Likewise, the distributor doesn't have access to the same information regarding the product with digital elements as the manufacturer and can only take such decisions on the ground of the information in its possession.	Keep this proposal The same provision should also apply to: • importer in article 13(6) and 13(9); • distributor in article 14(3), 14(4) and 14(6);
Product lifetime	IMCO	23(2)	35	The technical documentation shall be drawn up before the product with digital elements is placed on the market and shall be continuously updated, where appropriate, during the expected product lifetime or during a period of five years after the placing on the market of a product with digital elements, whichever is ***longer***	Negative	The expected lifetime should be freely determined by the manufacturer based on its technical capacities. For some technologies or types of products, it may be challenging for manufacturer to ensure sustainable and long-lasting products as the risks are constantly evolving and increasing. In these cases, while the level of resistance of the product with digital element can be estimated and guaranteed by the manufacturer over a medium period of	Revert to the proposal of the European Commission.

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
						time (3-5 years) **starting from the development of the product with digital elements, or the placement on the market of the first item,** it is hardly possible to guarantuee a product lifetime over 5 years, in particular for the items that are placed on the market long after their development. Multiple examples demonstrate this situation. Depending on the technologies, types of product, the risks, and the criticality, the manufacturer may be able to guarantee a more or less long lifetime, which in some cases may be below 5 years. Regarding the second modification, -the vulnerability handling also relies on the connectivity of the product with digital element, which is under control of the user, as well as its cooperation. if a serious issue is detected that makes the manufacturer decides that the best course of action is to discontinue the product. It's not clear what are the obligations of the manufacturer for the products on the field when they are not easy to be removed or the customer prefers to take the risk.	
Certificate management	IMCO	37(5)	40	Where, in the course of the monitoring of conformity following the issuance of a certificate, a notified body finds that a product no longer complies with the requirements laid down in this Regulation, it shall require the manufacturer to take appropriate corrective measures and shall ***restrict***, suspend or withdraw the certificate if necessary	Positive	The restriction of certificate was not listed here while it is envisioned in other articles	Keep this proposal specify "certificate of conformity" should be defined.
Market surveillance	IMCO	53(6)ca (new)	52	***The subsequent behaviour of the operator following information or***	Positive	The good faith, behaviour and especially attempts to take corrective actions of economic operators should also be	Keep this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				knowledge about the respective non-compliance		considered when deciding on the amount of the administrative fines. Therefore, such criteria should also be considered	
Market surveillance	IMCO	53(6a) (new)	53	***The respective authority may be empowered to apply fines below the minimum threshold when all of the following is observed:*** ***(a) the infringement is unintentional;*** ***(b) the infringement did not and is unlikely to result in negative consequences;*** ***(c) no administrative fines have previously been applied by the same of other market surveillance authorities to the same operator for a similar infringement during the previous three years;*** ***(d) upon coming to know about the respective non-compliance the operator employed all the appropriate corrective measures as well as reasonably necessary measures to avoid or minimise potential negative consequences.***	Positive	This proposal will support progressive administrative fines, taking into account the track record of the economic operator.	Keep this proposal
Entry into force	IMCO	57(2)	54	It shall apply from [***40*** months after the date of entry into force of this Regulation]. However, ***Chapter II, III, V and VII*** shall apply ***no earlier than [40*** months after the date of entry into force of this Regulation] ***as far as products with digital elements are concerned. As far as products with critical elements are concerned, Chapter II, III, V and VII shall apply no earlier than [20 months after the date of publication of the harmonised standards developed under the standardisation requires for the purpose of this Regulation].***	Negative	This proposal substantially postpones the implementation of the text. In addition the minimum timeframe of 20 months after publication of harmonised standard (hEN) for the application of Chapter II, III, V, VII is not necessary , as • Existing Industry Standard (EN) or Common specification on a respective vertical could be used instead • and could be published much earlier; • EU cybersecurity certificate could also be used as a mean	Remove this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
						to demonstrate conformity (under council revised version); To be applicable and to ensure legal certainty, definitions are necessary. - The Commission shall provide the definition of the products category, - The necessary element and format of the SBOM These elements should be defined ahead in advance of the entry into force of this regulation. Moreover, to ensure the correct activation of the provisions laid down in article 11, issuance of the implementing acts (art. 11.5) regarding the type of information, format and procedure of the notification are necessary.	
Common specifications	IMCO	57(2)	54	It shall apply from [***40*** months after the date of entry into force of this Regulation]. However, ***Chapter II, III, V and VII*** shall apply ***no earlier than [40*** months after the date of entry into force of this Regulation] ***as far as products with digital elements are concerned. As far as products with critical elements are concerned, Chapter II, III, V and VII shall apply no earlier than [20 months after the date of publication of the harmonised standards developed under the standardisation requires for the purpose of this Regulation].***	Negative	Common specifications should not discard as they may also be very useful to leverage existing industry or sector specific standards for which it has been demonstrated that they meet some or all of the essential requirements of Annex I. As such, common specification could support a quick implementation of the CRA, while limiting the impact on the industry.	Remove this proposal
Information and instructions to the user	IMCO	Annex II (1)5	56	***No later than 6 months after the date of entry into force of this Regulation, the Commission shall issue guidelines on how***	Negative	This provision should be maintained as it is a key information that should be made available to the user so that he can use	Remove this proposal

Topic	Actor	Art.	ADM #	Content	Impression	Comment	Proposal
				to apply the requirements in this Regulation to non-tangible products.		the product with digital element in a manner ensuring its cybersecurity.	
Skills	ITRE	29(7)	86	7a. Member States and the Commission shall put in place appropriate measures to ensure sufficient availability of skilled professionals, in order to minimise bottlenecks in the activities of conformity assessment bodies.	Positive with comments	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 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 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.	7a. Member States and the Commission shall put in place appropriate measures to ensure sufficient availability of skilled professionals ***in security domains***, in order to minimise bottlenecks in the activities of conformity assessment bodies.